Trend Micro Apex One™

Service Pack 1

管理者ガイド

Endpoint Security

Protected Cloud

Web Security

※注意事項

複数年契約について

・お客さまが複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。

・複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。

・各製品のサポート提供期間は以下の Web サイトからご確認いただけます。

https://success.trendmicro.com/jp/solution/000207383

法人向け製品のサポートについて

・法人向け製品のサポートの一部または全部の内容、範囲または条件は、トレンドマイクロの裁量により随時変更される場合があります。

・法人向け製品のサポートの提供におけるトレンドマイクロの義務は、法人向け製品サポートに関する合理的な努力を行うことに限られるものとします。

商標について

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDI オプション、おまかせ不正請求クリーンナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポートプレミアム、Air サポート、Connected Threat Defense、ライトクリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、Trend Micro Policy-based Security Orchestration、Writing Style DNA、Securing Your Connected World、Apex One、Apex Central、MSPL、TMOL、TSSL、ZERO DAY INITIATIVE、Edge Fire、Smart Check、Trend Micro XDR、Trend Micro Managed XDR、OT Defense Console、Edge IPS、Trend Micro Cloud One、スマスキャ、Cloud One、Cloud One - Workload Security、Cloud One - Conformity、ウイルスバスター チェック！、Trend Micro Security Master、Trend Micro Service One、

P/N: APEM09524/220511_JP (2022/08)

プライバシーと個人データの収集に関する規定

トレンドマイクロ製品の一部の機能は、お客さまの製品の利用状況や検出にかかわる情報を収集してトレンドマイクロに送信します。この情報は一定の管轄区域内および特定の法令等において個人データとみなされることがあります。トレンドマイクロによるこのデータの収集を停止するには、お客さまが関連機能を無効にする必要があります。

Trend Micro Apex One により収集されるデータの種類と各機能によるデータの収集を無効にする手順については、次の Web サイトを参照してください。

https://www.go-tm.jp/data-collection-disclosure

重要

データ収集の無効化やデータの削除により、製品、サービス、または機能の利用に影響が発生する場合があります。Trend Micro Apex One における無効化の影響をご確認の上、無効化はお客さまの責任で行っていただくようお願いいたします。

トレンドマイクロは、次の Web サイトに規定されたトレンドマイクロのプライバシーポリシー (Global Privacy Notice) に従って、お客さまのデータを取り扱います。

https://www.trendmicro.com/ja_jp/about/legal/privacy-policy-product.html

目次

パート II：セキュリティエージェントの保護

第 4 章：Trend Micro Smart Protection の使用

第 5 章：セキュリティエージェントのインストール

第 6 章：最新の保護状態の維持

第 7 章：セキュリティリスクの検索

第 8 章：未知の脅威からの保護

第 9 章：挙動監視の使用

第 10 章：デバイスコントロールの使用

第 11 章：情報漏えい対策の使用

第 12 章：Web レピュテーションの使用

付録 A：Apex One の IPv6 のサポート

付録 B：Windows Server Core のサポート

付録 C：用語集

索引

はじめに

このドキュメントでは、使用開始の手順、エージェントのインストール手順、および Apex One サーバとエージェントの管理について説明します。

この章は次のトピックで構成されます。

Apex One 付属のドキュメント

Apex One のドキュメントには、次のものが含まれます。

表 1. Apex One 付属のドキュメント

ドキュメント	説明
インストールガイド	Apex One サーバをインストールし、サーバとエージェントをバージョンアップするための要件および手順を説明した PDF ドキュメント 注意 マイナーリリースバージョン、Service Pack、または Patch にはインストールガイドが付属していない場合があります。
システム要件	Apex One サーバをインストールし、サーバとエージェントをバージョンアップするためのシステムの最小要件と推奨要件を説明した PDF ドキュメント
管理者ガイド	使用開始にあたっての情報、セキュリティエージェントのインストール手順、および Apex One サーバとエージェントの管理について説明した PDF ドキュメント
ヘルプ	操作手順、使用にあたってのアドバイス、および目的別の作業手順を提供する、WebHelp または CHM 形式のオンラインヘルプ。Apex One サーバ、エージェントコンソール、および Apex One のインストーラからアクセスできます。
Readme ファイル	既知の問題のリストと基本的なインストール手順が含まれています。ヘルプや関連ガイドには含まれない最新の製品情報も含まれる場合があります。
Apex One サポートページ	本 Web サイトでは、「よくあるお問い合わせ」、「製品 Q&A」、「サポートセンターへの問い合わせ」などの役立つ情報をご紹介していますのでご活用ください。 http://tmqa.jp/corp14-banner1

最新のドキュメントおよび Readme ファイルは、次の Web サイトからダウンロードできます。

http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

対象読者

Apex One 付属のドキュメントは、次のユーザを対象としています。

- Apex One 管理者: Apex One サーバおよびセキュリティエージェントのインストールと管理を含む Apex One 管理の責任者。ネットワーキングおよびサーバ管理についての高度な知識を持つユーザであることが想定されています。
- エージェントユーザ: エンドポイントにセキュリティエージェントをインストールしているユーザ。エンドポイントのスキルレベルは限定されず、コンピュータ初心者から上級ユーザまでを対象とします。

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表 2. ドキュメントの表記規則

表記	説明
 注意	設定上の注意
 ヒント	推奨事項
 重要	必須の設定や初期設定、および製品の制限事項に関する情報
 警告!	避けるべき操作や設定についての注意

用語

次の表は、Apex One 付属のドキュメントで使用されている正式な用語を示しています。

表 3. Apex One の用語

用語	説明
セキュリティエージェント	Apex One エージェントプログラム
エージェントエンドポイント	セキュリティエージェントがインストールされているエンドポイント
エージェントユーザ (またはユーザ)	エージェントエンドポイントでセキュリティエージェントを使用するユーザ
サーバ	Apex One サーバプログラム
サーバコンピュータ	Apex One サーバがインストールされているエンドポイント
管理者 (または Apex One 管理者)	Apex One サーバの管理者
コンソール	Apex One サーバおよびエージェントを設定および管理するためのユーザインタフェース。 Apex One サーバプログラム用のコンソールを「Web コンソール」、セキュリティエージェントプログラム用のコンソールを「セキュリティエージェントコンソール」と呼びます。
セキュリティリスク	ウイルス/不正プログラム、スパイウェア/グレーウェア、および Web からの脅威の総称
製品サービス	ウイルス対策、ダメージクリーンナップサービス、Web レピュテーションおよびスパイウェア対策を含みます。これらはすべて Apex One サーバのインストール時にアクティベートされます。
Apex One サービス	Microsoft 管理コンソール (MMC) によってホストされるサービス。たとえば、Apex One Master Service の `ofcservice.exe` などです。

用語	説明
プログラム	セキュリティエージェントやプラグインマネージャも含まれます。
コンポーネント	セキュリティ上の脅威の検索、検出、および処理を実行するものです。
エージェントインストールフォルダ	セキュリティエージェントのファイルが含まれるエンドポイント上のフォルダ。インストール時の初期設定では、インストールフォルダは次のいずれかの場所になります。 C:¥Program Files¥Trend Micro¥Security Agent C:¥Program Files (x86)¥Trend Micro¥Security Agent
サーバインストールフォルダ	Apex One サーバのファイルが含まれるエンドポイント上のフォルダ。インストール時の初期設定では、インストールフォルダは次のいずれかの場所になります。 C:¥Program Files¥Trend Micro¥Apex One C:¥Program Files (x86)¥Trend Micro¥Apex One たとえば、サーバのインストールフォルダで¥PCCSRV の下にあるファイルのフルパスは次のようになります。 C:¥Program Files¥Trend Micro¥Apex One¥PCCSRV¥<ファイル名>
スマートスキャンエージェント	スマートスキャンを使用するように設定されているセキュリティエージェント
従来型スキャンエージェント	従来型スキャンを使用するように設定されているセキュリティエージェント

用語	説明
デュアルスタック	IPv4 アドレスと IPv6 アドレスの両方を持つエンティティ。 例: ・ IPv4 アドレスと IPv6 アドレスの両方を持つエンドポイント ・ デュアルスタックエンドポイントにインストールされたセキュリティエージェント ・ エージェントにアップデートを配信するアップデートエージェント ・ IPv4 アドレスと IPv6 アドレスを変換できる、DeleGate などのデュアルスタックプロキシサーバ
IPv4 シングルスタック	IPv4 アドレスのみを持つエンティティ
IPv6 シングルスタック	IPv6 アドレスのみを持つエンティティ
プラグインソリューション	プラグインマネージャから配信される、Apex One に本来備わる機能およびプラグインプログラム

パート I

導入と使用開始

第 1 章

Apex One の概要

この章では、Trend Micro Apex One とその機能の概要について説明します。

この章は次のトピックで構成されます。

Apex One について

Trend Micro Apex One は、不正プログラム、ネットワークウイルス、Web ベースの脅威、スパイウェア、および複合型の脅威の攻撃から企業のネットワークを保護します。Apex One は、エンドポイントに配置されたセキュリティエージェントプログラムと、すべてのエージェントを管理するサーバプログラムで構成される統合ソリューションです。セキュリティエージェントはエンドポイントを保護し、エンドポイントのセキュリティステータスをサーバに報告します。サーバからは、Web ベースの管理コンソールを使用して、セキュリティポリシーの設定とアップデートの配信を各セキュリティエージェントに対して簡単に行えます。

Apex One は、Trend Micro Smart Protection Network と連動しています。Smart Protection Network は次世代のクラウド-クライアント型インフラストラクチャで、従来のアプローチよりも優れたセキュリティを実現します。独自のクラウドテクノロジとより軽量なクライアントを使用することで、パターンファイルのダウンロードに依存していた従来の負担を軽減し、デスクトップのアップデートに伴う一般的な延期を解消します。使用可能なネットワーク帯域幅の増加、処理電力の低減、および関連コストの削減によって、多くのビジネスにメリットがもたらされます。ユーザは、企業ネットワーク内、自宅、外出先のいずれの場所からでも、最新のセキュリティ対策を利用することができます。

新機能

次の表は、本バージョンの Trend Micro Apex One の新機能および機能強化を示しています。

表 1-1. Apex One Service Pack 1

項目	説明
プラットフォームのサポートの強化	Windows Server 2022 への Apex One サーバのインストールがサポートされます。

表 1-2. Apex One Patch 6

項目	説明
プラットフォームのサポートの強化	Windows 10 21H2、Windows 11、Windows Server 2022 へのセキュリティエージェントのインストールがサポートされます。

表 1-3. Apex One Patch 5

項目	説明
管理者通知の強化	管理者通知では、オプションの SSL/TLS 暗号化を使用した NTLM 認証がサポートされます。
セキュリティエージェントセルフプロテクション	セルフプロテクションの設定は自動的に有効になるため、設定できません。セルフプロテクション機能の以前の依存関係は削除され、すべてのセキュリティエージェントを常に保護できるようになりました。
プラットフォームのサポート	Windows 10 May 2021 Update (21H1) へのセキュリティエージェントのインストールがサポートされます。

表 1-4. Apex One Patch 4

項目	説明
SQL Server データベース設定ツール	SQL Server データベース設定ツールでは、Endpoint Sensor データベースの移動がサポートされます (Apex One データベースと同じ SQL Server にインストールされている場合)。
Endpoint Sensor	Endpoint Sensor は、設定した仮想アナライザにサンプル送信を行うように強化されました。
プラットフォームのサポートの強化	Windows 10 October Update (20H2) へのセキュリティエージェントのインストールがサポートされます。

表 1-5. Apex One Patch 3

項目	説明
パスワードの複雑さの強化	セキュリティを向上するために、セキュリティエージェントのアンロードおよびアンインストール機能におけるパスワードの複雑さの要件が強化されました。
プラットフォームのサポートの強化	Windows 10 May 2020 Update (20H1) へのセキュリティエージェントのインストールがサポートされます。

項目	説明
SQL Server のサポート	Apex One では SQL Server 2019 がサポートされます。

主要機能と利点

Apex One に含まれる主要な機能および利点は次のとおりです。

表 1-6. 主要機能と利点

機能	利点
ランサムウェア対策	検索機能が強化され、ランサムウェアプログラムに共通する動作を特定してそのプロセスをブロックすることにより、エンドポイントで実行される文書を標的としたランサムウェアプログラムを特定してブロックします。
Connected Threat Defense	Apex One で Apex Central サーバの不審オブジェクトリストを利用できます。Apex Central 管理コンソールを使用して、不審オブジェクトリストで検出されたオブジェクトに対して独自の処理を作成することができます。トレンドマイクロ製品で保護されているエンドポイントで検出された脅威に対し、環境に応じたカスタムの防御を実装できます。 まだ特定されていない脅威を含んでいる可能性があるファイルオブジェクトが検出された場合、詳しい分析のために仮想アナライザに送信するようにセキュリティエージェントを設定できます。オブジェクトが未知の脅威を含むと判定した場合、仮想アナライザはオブジェクトを不審オブジェクトリストに追加し、そのリストをネットワーク上の他のすべてのセキュリティエージェントに配信します。
プラグインマネージャとプラグインソリューション	プラグインマネージャを使用すると、プラグインソリューションを簡単にインストール、配信、および管理できます。 管理者は、次の 2 種類のプラグインソリューションをインストールできます。 • プラグインプログラム • 組み込みの Apex One 機能

機能	利点
一元管理	管理者は、Web ベースの管理コンソールからネットワーク上のすべてのエンドポイントやサーバに透過的にアクセスできます。Web コンソールでは、すべてのエンドポイントおよびサーバに対する、セキュリティポリシー、パターンファイル、およびソフトウェアアップデートの自動配信を管理できます。また大規模感染予防サービスにより、感染元をシャットダウンし、専用のセキュリティポリシーを迅速に配信して、パターンファイルが使用可能になるまでの間の大規模感染を防止および阻止します。Apex One は、リアルタイムの監視、イベント通知、および包括的なレポートの生成も行います。管理者は、リモートから管理業務を実行し、個々のエンドポイントやグループにカスタマイズしたポリシーを設定し、エンドポイントのセキュリティ設定をロックすることができます。
ウイルス対策/セキュリティリスク保護	Apex One は、ファイルを検索して、検出されたセキュリティリスクごとに特定の処理を実行することでセキュリティリスクからコンピュータを保護します。短期間に大量の数のセキュリティ上の脅威が検出された場合は大規模感染の兆候を示しています。Apex One は、大規模感染予防ポリシーを実行して、感染したコンピュータが完全に危険な状態でなくなるまで隔離することで大規模感染を抑制します。 Apex One では、スマートスキャンを使用して、より効率的な検索プロセスを実行します。スマートスキャンでは、これまでローカルのエンドポイントに保存されていた大量のシグネチャが Trend Micro Smart Protection ソースに移行されます。この手法により、増加し続けるシグネチャアップデートのエンドポイントシステムへの反映がシステムやネットワークに与える影響を著しく低減できます。 スマートスキャンおよびスマートスキャンをエージェントに導入する方法については、279 ページの「検索方法の種類」を参照してください。

機能	利点
ダメージクリーンナップサービス	ダメージクリーンナップサービスは、ファイルベースのコンピュータウイルス、ネットワークウイルス、およびウイルスやワームの残骸 (トロイの木馬、レジストリ侵入、ウイルスファイル) を完全に自動化されたプロセスを使用して駆除します。ダメージクリーンナップサービスでは、トロイの木馬の脅威および妨害に対して次のように対処します。 • 活動中のトロイの木馬を検出および削除 • トロイの木馬が作成したプロセスを中止 • トロイの木馬が変更したシステムファイルを修復 • トロイの木馬により作成されたファイルとアプリケーションを削除 ダメージクリーンナップサービスはバックグラウンドで自動的に実行されるので、設定の必要はありません。ユーザは実行されていることにすら気付きません。ただし、トロイの木馬を削除するプロセスを完了するために、エンドポイントの再起動を求められることがあります。
Web レピュテーション	Web レピュテーションテクノロジは、企業ネットワークの内部または外部に存在するエージェントエンドポイントを、予防措置によって不正な Web サイトや危険と考えられる Web サイトから保護します。Web レピュテーションにより感染経路は遮断され、不正コードのダウンロードも阻止されます。 Apex One を Smart Protection Server または Trend Micro Smart Protection Network と統合することで、Web サイトやページの信頼性を確認します。
Apex One ファイアウォール	Apex One ファイアウォールは、ステートフルインスペクションおよび高性能なネットワークウイルス検索機能を使用して、ネットワーク上のエンドポイントとサーバを保護します。 アプリケーション、IP アドレス、ポート番号、プロトコルなどによって接続をフィルタする複数のルールを作成し、それらのルールを異なるユーザのグループに適用します。

機能	利点
情報漏えい対策	情報漏えい対策は、組織のデジタル資産を不慮の流失や意図的な漏えいから守ります。情報漏えい対策により、管理者は次のことを実行できます。 • 保護するデジタル資産の特定 • メールメッセージや外部デバイスなどの一般的な転送チャネルを通したデジタル資産の転送を制限または阻止するポリシーの作成 • 制定されたプライバシー標準へのコンプライアンスの実施
デバイスコントロール	デバイスコントロールは、エンドポイントに接続された外部ストレージデバイスやネットワークリソースへのアクセスを制御します。デバイスコントロール機能により、データの損失や漏えいを防ぐことができ、またファイル検索と併用することでセキュリティリスクからの保護が実現されます。
挙動監視	挙動監視機能は、エンドポイントの OS またはインストールされたソフトウェアに対して不審な変更が行われていないかどうかを常に監視します。

Apex One サーバ

Apex One サーバは、すべてのエージェント設定、セキュリティリスクログ、およびアップデートを一元的に管理するリポジトリです。

サーバは、次の 2 つの重要な機能を実行します。

- セキュリティエージェントのインストール、監視、および管理
- エージェントに必要なコンポーネントのダウンロード。Apex One サーバは、トレンドマイクロのアップデートサーバからコンポーネントをダウンロードし、エージェントに配信します。

注意

一部のコンポーネントは Trend Micro Smart Protection ソースによってダウンロードされます。詳細については、106 ページの「Trend Micro Smart Protection ソース」を参照してください。

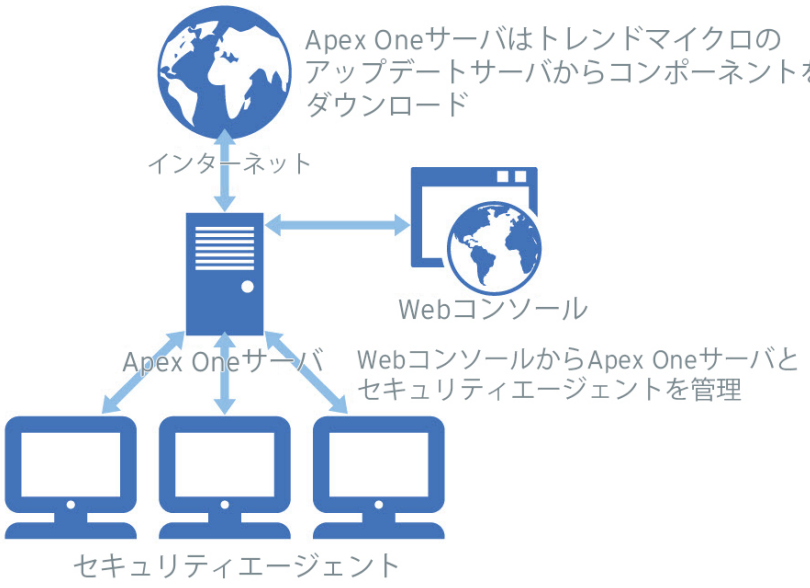


図 1-1. Apex One サーバの動作

Apex One サーバは、サーバとセキュリティエージェント間にリアルタイムの双方向通信を提供します。管理者は、ネットワーク上のどこからでも Web コンソールにアクセスでき、エージェントを管理できます。サーバは、HTTPS 経由でエージェントと通信します。

セキュリティエージェント

それぞれのエンドポイントにセキュリティエージェントをインストールすることで、セキュリティ上の脅威から Windows エンドポイントを保護します。

セキュリティエージェントは、親サーバにステータスを報告します。エージェント移動ツールを使用して、別のサーバに通知するようエージェントを設定することもできます。セキュリティエージェントは、イベントおよびステータス情報をリアルタイムでサーバに送信します。イベントには、ウイル

ス/不正プログラムの検出、セキュリティエージェントの起動、セキュリティエージェントの終了、検索の開始、アップデートの完了などがあります。

トレンドマイクロ製品およびサービスとの統合

Apex One は、次の表に記載されているトレンドマイクロ製品およびサービスと統合されます。シームレスな統合を実現するには、必要なバージョンまたは推奨バージョンが製品で実行されていることを確認してください。

表 1-7. Apex One と統合される製品およびサービス

製品/サービス	説明	バージョン
トレンドマイクロのアップデートサーバ	セキュリティ上の脅威からエンドポイントを保護するために必要なすべてのコンポーネントを提供します。	なし
Trend Micro Smart Protection Network	ファイルレピュテーションサービスおよび Web レピュテーションサービスをエージェントに提供します。 Trend Micro Smart Protection Network はトレンドマイクロによって管理されます。	なし
スタンドアロン Smart Protection Server	Trend Micro Smart Protection Network と同じファイルレピュテーションサービスおよび Web レピュテーションサービスを提供します。 スタンドアロンの Smart Protection Server は、サービスを企業ネットワーク内に導入することで効率を最適化することを目的としています。 **注意** 統合 Smart Protection Server は、Apex One サーバとともにインストールされます。スタンドアロンの Smart Protection Server と同じ機能を備えていますが、容量に制限があります。	• 3.3

製品/サービス	説明	バージョン
Apex Central	プラットフォームや、プログラムの物理的な場所に関係なく、ウイルス対策/コンテンツセキュリティプログラムを 1 か所で制御する機能を提供するソフトウェア管理ソリューションです。	• すべてのバージョン
Trend Micro Control Manager		• 7.0 Patch 1
Deep Discovery Analyzer	Deep Discovery は、カスタムサンドボックスと適切なリアルタイムインテリジェンスを備え、ネットワーク全体の監視を提供しています。これにより、攻撃の早期検出と迅速な抑制が可能になり、またカスタムのセキュリティアップデートにより、さらなる攻撃に対する保護が瞬時に強化されます。	5.1 以降

第 2 章

Apex One の使用開始

この章では、Trend Micro Apex One の使用を開始して、初期設定を実施する方法について説明します。

この章は次のトピックで構成されます。

Web コンソール

Web コンソールは、組織ネットワークを通して Apex One を監視するための中心点です。コンソールには一連の初期設定と値が搭載されており、セキュリティ要件と仕様に基づき設定を行うことができます。Web コンソールは、JavaScript、CGI、HTML、および HTTPS などの、標準のインターネットテクノロジを使用します。

注意

Web コンソールからタイムアウト設定を指定します。

詳細については、632 ページの「Web コンソールの設定」を参照してください。

Web コンソールを使って、以下を実行できます。

- ネットワーク上のエンドポイントにインストールされたエージェントを管理
- エージェントを論理ドメインにグループ分けして同時設定と管理を実行
- 検索設定をセットして、単一または複数のネットワーク上のエンドポイントで手動検索を開始
- ネットワーク上のセキュリティリスクに関する通知を設定し、エージェントから送信されたログを表示
- アウトブレークの基準と通知を設定
- 役割およびユーザアカウントの設定により他の Apex One 管理者に Web コンソール管理タスクを委任
- エージェントのセキュリティガイドラインへの準拠

注意

Web コンソールは、Windows UI モードでの Windows 8、Windows 8.1、Windows 10、または Windows Server 2012 をサポートしません。

Web コンソールを開くための要件

次のリソースを持つ、ネットワーク上の任意のエンドポイントから Web コンソールを開きます。

- 300MHz Intel Pentium または同等の CPU
- 128MB の RAM
- 30MB 以上のハードディスク空き容量
- 解像度 1366x768、256 色以上をサポートするモニタ
- Web ブラウザのサポート:
  - Microsoft Internet Explorer™ 10.0 以降
  - Microsoft Edge (レガシ/Chromium エディション)
  - Chrome

注意

Apex One では、Web コンソールを表示するためにのみ HTTPS トラフィックをサポートします。

Web ブラウザで、Apex One サーバのインストールの種類に基づき、アドレスバーに次のいずれかを入力します。

表 2-1. Web コンソールの URL

インストールの種類	URL
既定サイトに SSL がある	`https://<Apex One サーバの FQDN または IP アドレス>/Apex One`
仮想サイトに SSL がある	`https://<Apex One サーバの FQDN または IP アドレス>:<ポート番号>/Apex One`

注意

旧バージョンのサーバからバージョンアップした場合、Web ブラウザおよびプロキシサーバのキャッシュファイルが原因で、Apex One の Web コンソールが正常に読み込まれない場合があります。Web コンソールに正常にアクセスするには、ブラウザのキャッシュメモリ、および Apex One サーバとお使いのエンドポイントの間に配置されたすべてのプロキシサーバのキャッシュメモリを消去してください。

ログオンアカウント

Apex One サーバのインストール時、セットアップによってルートアカウントが作成され、このアカウントのパスワードを入力するよう求められます。初めて Web コンソールを開く場合は、ユーザ名に「root」と入力して、このルートアカウントのパスワードを入力します。パスワードを忘れた場合は、パスワードの再設定についてサポート担当者にお問い合わせください。

ユーザの役割を定義し、ユーザアカウントを設定して、他のユーザがルートアカウントを使用せずに Web コンソールにアクセスできるようにします。ユーザは、コンソールにログオンする際、各自に設定されたユーザアカウントを使用できます。詳細については、575 ページの「役割ベースの管理」を参照してください。

Web コンソールのバナー

Web コンソールのバナー領域には、次が表示されます。

- <アカウント名>: パスワードなど、このアカウントの詳細を変更するにはアカウント名 (例: root) をクリックします。
- ログオフ: Web コンソールからログオフします。

ヘルプ情報へのアクセス

[ヘルプ] メニューから次のサポート情報を確認できます。

- 目次とキーワード: オンラインヘルプが開きます。

- サポート情報: トレンドマイクロのサポート情報ページが表示されます。ここでは、質問を送信したり、トレンドマイクロ製品に関する一般的な質問への回答を見つけることができます。
- 脅威データベース: 不正プログラム関連情報のトレンドマイクロのリポジトリである脅威データベース Web サイトが表示されます。トレンドマイクロの脅威に関するエキスパートが、不正プログラム、スパム、不正な URL、脆弱性についての検出を定期的に公開しています。脅威データベースでは、注目度の高い Web 攻撃についても説明し、関連情報を提供しています。
- トレンドマイクロお問い合わせ先: 世界各国のオフィスに関する情報を含むトレンドマイクロのお問い合わせ Web サイトが表示されます。
- バージョン情報: 製品の概要、コンポーネントのバージョンの詳細をチェックする方法、およびインテリジェントシステムのサポートへのリンクが記載されたページが表示されます。

  詳細については、776 ページの「インテリジェントシステムのサポート」を参照してください。

ダッシュボード

Apex One Web コンソールを開くかメインメニューで ダッシュボード をクリックすると、ダッシュボード が表示されます。

Web コンソールのユーザアカウントはそれぞれ、完全に独立したダッシュボードを使用できます。あるユーザアカウントのダッシュボードを変更しても、他のユーザアカウントのダッシュボードには影響しません。

ダッシュボードに表示される Apex One のエージェントデータは、ユーザアカウントのエージェントドメインに対する権限によって異なります。たとえば、あるユーザアカウントにドメイン A および B を管理する権限を付与した場合、このユーザアカウントのダッシュボードには、ドメイン A および B に属するエージェントのデータのみが表示されます。

ユーザアカウントの詳細については、575 ページの「役割ベースの管理」を参照してください。

ダッシュボード 画面には次の項目が表示されます。

- 製品ライセンスのステータスセクション
- ウィジェット
- タブ

製品ライセンスのステータスセクション

このセクションは、ダッシュボードの上部にあり、Apex One のライセンスステータスが表示されます。

次の場合、ライセンスのステータスに関するメッセージが表示されます。

- 製品版ライセンスを使用しているとき
  - サポート契約の有効期限の 60 日前である場合。
  - 製品のサポート契約更新猶予期間である場合: 更新猶予期間については、トレンドマイクロの販売代理店にお問い合わせください。
  - サポート契約の有効期限が切れ、サポート契約更新猶予期間が経過した場合: この間、テクニカルサポートを受けたり、コンポーネントのアップデートを実行することはできません。その場合、検索エンジンでは、古いバージョンのパターンファイルを使用して検索が行われます。これらの旧版コンポーネントでは、最新のセキュリティリスクから完全には保護できない可能性があります。
- 体験版ライセンスを使用しているとき
  - 体験版ライセンスの有効期限の 14 日前である場合。
  - 体験版ライセンスの有効期限が切れた場合: Apex One では、コンポーネントのアップデート、検索、およびすべての製品機能が無効になります。

アクティベーションコードを取得している場合は、[管理] > [設定] > [製品ライセンス] に移動して製品版ライセンスにアップデートしてください。

製品情報バー

Apex One ではダッシュボード画面上部にさまざまなメッセージが表示され、管理者は追加情報を確認できます。

表示される情報は次のとおりです。

- Apex One の最新の Service Pack または Patch

  注意

  トレンドマイクロのダウンロードセンター (https://downloadcenter.trendmicro.com) から Patch をダウンロードするには、[詳細情報] をクリックしてください。

- 新しいウィジェット
- 契約の有効期限が近い場合の契約期間に関する通知
- 正規ライセンスかどうかの通知

  注意

  Apex One に使用されているライセンスが正規ライセンスでない場合、情報メッセージが表示されます。正規ライセンスを取得しないと、警告が表示され、アップデートの実行が停止されます。

タブとウィジェット

ウィジェットは、ダッシュボードの中核的なコンポーネントです。ウィジェットには、さまざまなセキュリティ関連イベントに関する詳細情報が表示されます。ウィジェットの中には、古いコンポーネントの更新などのタスクを実行できるものもあります。

ウィジェットに表示される情報は次のコンポーネントから収集されます。

- Apex One サーバと エージェント
- プラグインソリューションとそのエージェント
- Trend Micro Smart Protection Network

注意

スマートフィードバックを有効にして、Trend Micro Smart Protection Network からのデータを表示してください。スマートフィードバックの詳細については、636 ページの「スマートフィードバック」を参照してください。

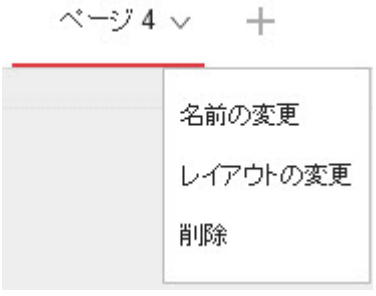
タブはウィジェットを表示するフレームです。ダッシュボードには最大 30 タブまで表示できます。

タブの操作

タブの管理タスクには、追加、名前変更、レイアウト変更、削除、タブ表示の自動切り替えがあります。

手順

1. ダッシュボードに移動します。
2. 新しいタブを追加するには、次の手順を実行します。
   a. 追加アイコンをクリックします。
   b. 新しいタブの名前を入力します。
3. タブの名前を変更するには、次の手順を実行します。
   a. タブ名にマウスを重ね、下矢印をクリックします。



b. [名前の変更] をクリックし、新しい名前を入力します。

4. タブのウィジェットのレイアウトを変更するには、次の手順を実行します。

   a. タブ名にマウスを重ね、下矢印をクリックします。

   b. [レイアウトの変更] をクリックします。

   c. 表示される画面で新しいレイアウトを選択します。

   d. [保存] をクリックします。

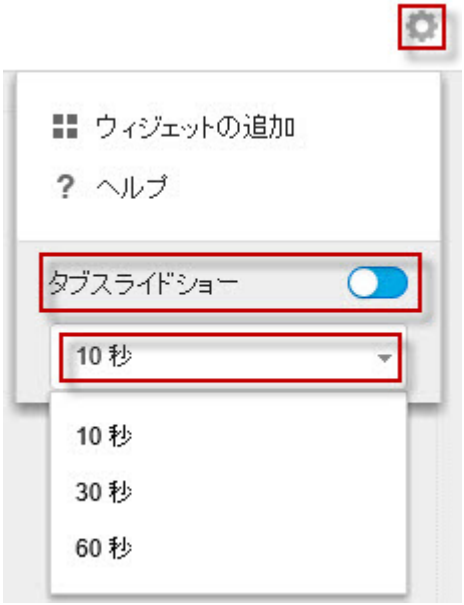
5. タブを削除するには、次の手順を実行します。

   a. タブ名にマウスを重ね、下矢印をクリックします。

   b. [削除] をクリックし、処理を確認します。

6. タブスライドショーを再生するには、次の手順を実行します。

   a. タブ表示の右にある [設定] ボタンをクリックします。



b. [タブスライドショー] コントロールを有効にします。

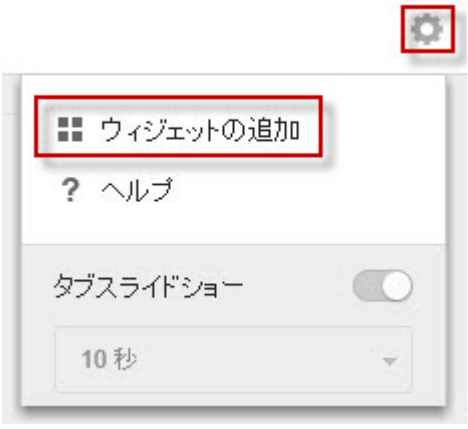
c. タブ表示を次のタブに切り替える間隔を選択します。

ウィジェットの操作

ウィジェットの管理タスクには、項目の追加、移動、サイズ変更、名前変更、削除があります。

手順

1. ダッシュボードに移動します。
2. タブをクリックします。
3. ウィジェットを追加するには、次の手順を実行します。
   a. タブ表示の右にある [設定] ボタンをクリックします。



   b. [ウィジェットの追加] をクリックします。
   c. 追加するウィジェットを選択します。
      - ウィジェット上部のドロップダウンからカテゴリを選択すると、ウィジェットを絞り込むことができます。

- 画面上部の検索テキストボックスを使用すると個別のウィジェットを検索できます。

d. [追加] をクリックします。

4. ウィジェットを同じタブの別の位置に移動するには、ウィジェットを新しい位置にドラッグアンドドロップします。
5. 複数列構成のタブでウィジェットのサイズを変更するには、カーソルをウィジェットの右端にポイントして、カーソルを左右に動かします。
6. ウィジェットの名前を変更するには、次の手順を実行します。
   a. 設定アイコン (>) をクリックします。
   b. 新しいタイトルを入力します。

      注意

      Apex One とプラグインの統合管理などの一部のウィジェットでは、ウィジェット関連の項目を変更できます。

   c. [保存] をクリックします。
7. ウィジェットを削除するには、削除アイコン (>) をクリックします。

[概要] タブのウィジェット

[概要] タブには、ネットワーク上のすべてのセキュリティエージェントのセキュリティステータスの概要が表示されます。

注意

[概要] タブに表示されるウィジェットは、追加、削除、変更できません。

使用可能なウィジェット:

- 46 ページの「脅威検出およびポリシー違反ウィジェット」
- 47 ページの「エンドポイントステータスウィジェット」

- 48 ページの「ランサムウェア概要ウィジェット」
- 50 ページの「検出数上位のランサムウェアウィジェット」
- 51 ページの「セキュリティリスク検出の推移ウィジェット」

脅威検出およびポリシー違反ウィジェット

このウィジェットには、過去 24 時間にネットワークで検出されたすべての脅威とポリシー違反の概要が表示されます。

脅威または違反の件数にマウスを重ねると、それぞれの内訳が表示されます。特定の機能のログを表示するには、右側の数字をクリックします。

表 2-2. 検出カテゴリ

カテゴリ	説明
既知の脅威	トレンドマイクロで確認済みのセキュリティの脅威が以下の分類別に表示されます。 • ウイルス/不正プログラム • スパイウェア/グレーウェア • Web レピュテーション
不明な脅威	高度なヒューリスティクス、分析、または機能モデリングを使用して検出された潜在的な脅威が、以下の分類別に表示されます。 • 機械学習型検索 • 挙動監視 • 不審接続監視 • 不審ファイルオブジェクト
ポリシー違反	会社のセキュリティ基準に対するポリシー違反が、以下の分類別に表示されます。 • ファイアウォール • デバイスコントロール • 情報漏えい対策

エンドポイントステータスウィジェット

このウィジェットには、ネットワーク上のセキュリティエージェントの接続およびアップデートステータスの概要、および Apex One サーバにレポートしない管理対象外エンドポイントの数が表示されます。

件数にマウスを重ねると、内訳が表示されます。特定のステータスのログを表示するには、右側の数字をクリックします。

表 2-3. エージェント/エンドポイントグループ

グループ	説明
管理対象エージェント	ネットワーク上のセキュリティエージェントの最後にレポートされた接続状態が表示されます。 ・ オンライン ・ オフライン ・ スタンドアロン
旧版のエージェント	コンポーネントのカテゴリと、各カテゴリで旧版のコンポーネントを使用しているセキュリティエージェントの数が表示されます。

グループ	説明
管理対象外のエンドポイント	Apex One で検出できるすべてのエンドポイントのうち、セキュリティエージェントプログラムがインストールされていないエンドポイントまたは Apex One サーバにレポートしていないエンドポイントのリストが表示されます。 注意 管理対象外のエンドポイントの数が Apex One サーバで定期的にアップデートされるようにするには、次の手順を実行します。 1. 診断する Active Directory/IP アドレス範囲を定義します。 詳細については、59 ページの「Active Directory 統合」を参照してください。 2. 予約診断を設定します。 詳細については、707 ページの「管理対象外のエンドポイントに関するセキュリティコンプライアンス」を参照してください。

ランサムウェア概要ウィジェット

このウィジェットには、指定した期間に試行されたすべてのランサムウェアの概要が表示されます。

初期設定の表示では、検出されたすべてのランサムウェアの概要が感染経路ごとに分類されて表示されます。

- 初期設定の表示でランサムウェアの検出数をクリックすると、[セキュリティリスク - ランサムウェアログ] 画面に検出されたランサムウェアの詳細が表示されます。

ウィジェット右側にあるグラフをクリックすると、グラフデータが拡大されて表示されます。

- 特定の日付のデータにマウスを重ねると、表示されている検出カテゴリの検出総数が表示されます。データをクリックすると、[セキュリティリスク - ランサムウェアログ] 画面が表示され、その日に検出されたランサムウェアの詳細が表示されます。

表 2-4. ランサムウェア検出チャネル

チャネル	説明	検索の種類
Web	Web クライアント (ブラウザや FTP クライアントなど) でダウンロードされたファイル	• Web レピュテーション • リアルタイム検索 • 挙動監視
ネットワークトラフィック	不審接続監視機能で検出されたランサムウェア	• 不審接続監視
クラウド同期	サポート対象の次のクラウドストレージサービスによってローカルの同期フォルダに同期されたファイル • Microsoft™ OneDrive™	• リアルタイム検索 • 挙動監視 • 機械学習型検索
メール	Microsoft Outlook で開かれたメールの添付ファイル **注意** その他のメールクライアントアプリケーションで開かれた添付ファイルは、すべて [ローカルまたはネットワークドライブ] に分類されます。	• リアルタイム検索 • 挙動監視
自動実行ファイル	リムーバブルストレージドライブにあるプログラムのうち自動実行ファイルで実行されたプログラム **注意** リムーバブルストレージデバイスにあるファイル/プログラムのうち、自動実行プログラムで実行されていないものは、すべて [ローカルまたはネットワークドライブ] に分類されます。	• リアルタイム検索 • 挙動監視

チャネル	説明	検索の種類
ローカルまたはネットワークドライブ	ローカルまたはネットワークドライブで検出された以下のランサムウェア • Microsoft Outlook 以外のメールクライアントで開かれたメールの添付ファイル • リムーバブルストレージデバイスにあるファイルのうち自動実行プログラムで実行されていないファイル	• リアルタイム検索 • 手動検索 • 予約検索 • ScanNow • 挙動監視

セキュリティ脅威 - ランサムウェアログ

セキュリティ上の脅威 - ランサムウェアログでは、脅威を検出した検索の種類に関係なく、ネットワークで検出されたすべてのランサムウェアの脅威の概要を確認できます。

項目	説明
日時	検出された日時
セキュリティ上の脅威	セキュリティ上の脅威の名前
カテゴリ	脅威を検出した検索の種類
ファイルパス/URL	脅威の検出が行われた場所、または不正な Web サイトの検出に使用されたリスト
処理	脅威に対して実行された処理
感染経路	脅威の感染経路
エンドポイント	検出が行われたエンドポイント

検出数上位のランサムウェアウィジェット

このウィジェットには、指定した期間に検出された上位のランサムウェアの概要が表示されます。

ドロップダウンリストを使用して、表示するランサムウェアデータの種類を選択します。

表示	説明
エンドポイント	ネットワークでランサムウェアの検出数が多い上位のエンドポイントが表示されます。 ランサムウェアの検出数をクリックすると、[セキュリティリスク - ランサムウェアログ] 画面に検出されたランサムウェアの詳細が表示されます。
ランサムウェアの種類	ネットワークで検出数が多い上位のランサムウェアの種類が表示されます。 [脅威名] のリンクをクリックすると、トレンドマイクロの脅威データベースが開き、特定の脅威の種類に関する詳しい情報を確認できます。
ドメイン	ネットワークで検出数が多い上位のランサムウェアドメインが表示されます。 [脅威名] のリンクをクリックすると、トレンドマイクロの脅威データベースが開き、特定のドメインに関する詳しい情報を確認できます。

セキュリティリスク検出の推移ウィジェット

このウィジェットには、ネットワーク上のエンドポイントでの一定期間における脅威の検出状況とそれらの脅威の種類に関する概要が表示されます。

[感染エンドポイント] ボタンまたは [脅威の種類] ボタンをクリックすると、表示が切り替わります。

表示	説明
感染エンドポイント	指定した期間に脅威またはポリシー違反が検出されたエンドポイントの日別の傾向が表示されます。

表示	説明
脅威の種類	指定した期間にログに記録された脅威およびポリシー違反の数がグラフ形式で表示されます。 • グラフの下から脅威の種類をクリックすると、グラフ上の対応する検出情報の表示/非表示が切り替わります。 • 特定の日付のデータにマウスを重ねると、表示されている脅威の種類の検出総数が表示されます。データをクリックすると、リストで強調表示された脅威の種類のログ画面が表示されます。

ヒント

このウィジェットは、複数追加して両方の画面を表示できます。

情報漏えい対策オプションのウィジェット

注意

情報漏えい対策オプションのウィジェットは、Apex One 情報漏えい対策オプションをアクティベートすると使用できるようになります。

使用可能なウィジェット:

情報漏えい対策イベントの推移ウィジェット

このウィジェットには、一定期間における情報漏えい対策イベントの総数が表示されます。

注意

実行された処理 (「ブロック」または「放置」) に関係なく、すべての情報漏えい対策イベントの検出数が表示されます。

情報漏えい対策の上位イベントウィジェット

このウィジェットには、指定した期間に情報漏えい対策イベントを実行した上位のユーザ、チャネル、テンプレート、またはエンドポイントが表示されます。

注意

- このウィジェットには、最大で 10 件のユーザ、チャネル、テンプレート、またはエンドポイントが表示されます。
- 実行された処理 (「ブロック」または「放置」) に関係なく、すべての情報漏えい対策イベントの検出数が表示されます。

[表示基準] ドロップダダウンを使用して、表示する情報漏えい対策データの種類を選択します。

表 2-5. 情報漏えい対策の表示

表示	説明
ユーザ	デジタル資産の転送数が多い上位のユーザ • グラフの下にあるユーザ名をクリックすると、グラフ上の対応する検出情報の表示と非表示が切り替わります。 • 検出数のバーにマウスを重ねると、ユーザ名とそのユーザの情報漏えい対策イベント数が表示されます。
チャネル	デジタル資産の転送に最も多く使用されたチャネル • グラフの下にあるチャネル名をクリックすると、グラフ上の対応する検出情報の表示と非表示が切り替わります。 • 検出数のバーにマウスを重ねると、チャネル名とそのチャネルの情報漏えい対策イベント数が表示されます。
テンプレート	最も多く検出を実行したデジタル資産のテンプレート • グラフの下にあるテンプレート名をクリックすると、グラフ上の対応する検出情報の表示と非表示が切り替わります。 • 検出数のバーにマウスを重ねると、テンプレート名とそのテンプレートの情報漏えい対策イベント数が表示されます。

表示	説明
エンドポイント	デジタル資産の転送数が多い上位のエンドポイント • グラフの下にあるエンドポイント名をクリックすると、グラフ上の対応する検出情報の表示と非表示が切り替わります。 • 検出数のバーにマウスを重ねると、エンドポイント名とそのエンドポイントの情報漏えい対策イベント数が表示されます。

Apex One のウィジェット

Apex One のウィジェットでは、セキュリティエージェントのセキュリティステータスや検出状況、プラグインプログラムの情報、アウトブレークの発生状況をすばやく確認できます。

使用可能なウィジェット:

C&C コールバックイベントウィジェット

このウィジェットには、攻撃対象や送信元のコールバックアドレスを含む、C&C コールバックイベント情報が表示されます。

特定の C&C サーバリストから表示する C&C コールバック情報を選択できます。リストのソース (グローバルインテリジェンス、仮想アナライザ) を選択するには、ウィジェット設定アイコン (>) をクリックし、[C&C リストのソース] ドロップダウンからリストを選択します。

[表示順] ドロップダウンリストを使用して、表示する C&C コールバックデータの種類を選択します。

- 感染ホスト:最新の C&C 情報を対象のエンドポイントごとに表示

表 2-6. 感染ホストの情報

列	説明
感染ホスト	C&C 攻撃の対象となったエンドポイント名

列	説明
コールバックアドレス	エンドポイントが接続を試行したコールバックアドレスの数
最新コールバックアドレス	エンドポイントが接続を試行した最新のコールバックアドレス
コールバック回数	対象のエンドポイントがコールバックアドレスへの接続を試行した回数 注意 ハイパーリンクをクリックして [C&C コールバックログ] 画面を開くと、詳細情報が表示されます。

- コールバックアドレス:最新の C&C 情報を C&C コールバックアドレスごとに表示

表 2-7. C&C アドレス情報

列	説明
コールバックアドレス	ネットワークから発生した C&C コールバックのアドレス
C&C リスクレベル	グローバルインテリジェンスまたは仮想アナライザリストにより特定された、コールバックアドレスのリスクレベル
感染ホスト	コールバックアドレスの対象となったエンドポイントの数
最新感染ホスト	C&C コールバックアドレスへの接続を最近試行したエンドポイントの名前
コールバック回数	ネットワークからアドレスに対して試行されたコールバックの回数 注意 ハイパーリンクをクリックして [C&C コールバックログ] 画面を開くと、詳細情報が表示されます。

セキュリティリスクの検出 ウィジェット

このウィジェットには、検出されたセキュリティリスクの数と感染エンドポイントの数が表示されます。

エンドポイント数をクリックすると、[エージェント管理] 画面が開き、エージェントツリー内の感染したセキュリティエージェントのリストが表示されます。

Apex One とプラグインの統合管理 ウィジェット

このウィジェットでは、セキュリティエージェントからのデータとインストールされたプラグインプログラムとのデータが結合され、データがエージェントツリーに表示されます。このウィジェットによって、エージェントの保護範囲を迅速に診断できるため、個々のプラグインプログラムの管理に必要となる作業負荷を削減できます。

このウィジェットには、次のプラグインプログラムのデータが表示されます。

- Trend Micro VDI オプション

重要

統合管理ウィジェットで対応するデータを表示するには、サポートされるプラグインプログラムをアクティベートしておく必要があります。これらのプラグインプログラムの新しいバージョンが使用可能な場合にはバージョンアップします。

エージェントツリーに表示される列を選択するには、ウィジェットの右上にある [その他のオプション] ボタンをクリックし、[ウィジェット設定] ボタンをクリックします。

任意の列のデータをクリックすると、対応するプラグインプログラムのコンソール、または Apex One の [エージェント管理] 画面が開きます。表示される画面は、クリックしたデータの種類によって異なります。

ウイルス対策エージェントの接続状態ウィジェット

このウィジェットには、セキュリティエージェントから Apex One サーバへの接続状態が、設定されている検索方法 (スマートスキャンおよび従来型スキャン) ごとに表示されます。

表示アイコン ( ) をクリックして、表と円グラフのどちらでデータを表示するかを選択できます。

表示されるデータの種類を変更するには、表またはグラフの上にあるドロップダウンリストを使用します。ステータスの横の数をクリックすると、[エージェント管理] 画面が開き、エージェントツリー内の関連するセキュリティエージェントのリストが表示されます。

表示	説明
すべて	両方の検索方法について、すべてのセキュリティエージェントの接続状態が表示されます。
従来型スキャン	従来型スキャンを使用するすべてのセキュリティエージェントの接続状態が表示されます。
スマートスキャン	スマートスキャンを使用するすべてのセキュリティエージェントの接続状態が表示されます。 エージェントの接続状態を表で表示する場合は次のようになります。 • 「オンライン」のエージェントの情報を展開すると、Smart Protection Server との接続状態が表示されます。 • URL をクリックすると、Smart Protection Server の管理コンソールが開きます。 注意 Smart Protection Server との接続状態を報告できるのは、オンラインエージェント (Apex One サーバに報告するエージェント) のみです。 オフラインエージェントの Smart Protection Server との接続を復元する方法については、677 ページの「セキュリティエージェントアイコンが示す問題の解決方法」を参照してください。

エッジリレーサーバへのエージェント接続状況ウィジェット

このウィジェットには、一定期間に Apex One エッジリレーサーバに接続されたセキュリティエージェントの数が表示されます。

アウトブレークウィジェット

アウトブレークウィジェットには、現在発生しているすべてのアウトブレークアラートと前回のアウトブレークアラートのステータスが表示されます。

- アラートの日時をクリックすると、アウトブレークの詳細が表示されます。
- Apex One でアウトブレークが検出されたら、アウトブレークアラート情報のステータスをリセットして、ただちに大規模感染予防策を実行してください。

  大規模感染予防策の実行方法の詳細については、383 ページの「大規模感染予防ポリシー」を参照してください。
- [セキュリティリスクトップ 10 の表示] をクリックすると、最も蔓延しているセキュリティリスク、最も多くセキュリティリスクが検出されたエンドポイント、および上位の感染源を表示できます。

[セキュリティリスクトップ 10] 画面では、次の操作が可能です。

- セキュリティリスク名をクリックすると、セキュリティリスクに関する詳細情報が表示されます。
- エンドポイント名をクリックすると、特定のエンドポイントの全体的なステータスが表示されます。
- エンドポイント名に対応する [表示] をクリックすると、そのエンドポイントのセキュリティリスクログが表示されます。
- [リセット] をクリックすると、各表の統計情報がリセットされます。

エージェントのアップデート状況ウィジェット

このウィジェットには、セキュリティエージェントをセキュリティリスクから保護するために使用可能なコンポーネントとプログラムが表示されます。

「旧版」列をクリックすると、[エージェント管理] 画面が開き、エージェントツリー内のアップデートが必要なセキュリティエージェントのリストが表示されます。

管理ウィジェット

管理ウィジェットには、セキュリティエージェントの Apex One サーバとの接続状態が表示されます。

使用可能なウィジェット:

エージェントとサーバの接続状態ウィジェット

このウィジェットには、すべてのエージェントと Apex One サーバとの接続状態が表示されます。

表示アイコン () をクリックすると、表と円グラフの表示を切り替えることができます。

ステータスの横の数をクリックすると、[エージェント管理] 画面が開き、エージェントツリー内の関連するセキュリティエージェントのリストが表示されます。

Active Directory 統合

Apex One を Microsoft™ Active Directory™構造に統合することにより、セキュリティエージェントを効率良く管理し、Active Directory アカウントを使用して Web コンソールの権限を割り当て、セキュリティソフトウェアがインストールされていないエージェントを特定することができます。ネットワークドメイン内のすべてのユーザは、Apex One コンソールに安全にアクセスできます。別のドメイン内のユーザであっても、特定のユーザに、制限されたアクセスが可能になるよう設定することもできます。ユーザのアカウント情報は、認証プロセスと暗号化キーによって検証されます。

Active Directory との統合により、次のようなメリットがあります。

- カスタムエージェントグループ: Active Directory または IP アドレスを使用して、エージェントを手動でグループ化し、Apex One エージェントツリーのドメインにマップします。

  詳細については、74 ページの「エージェントの自動グループ設定」を参照してください。

- 管理対象外のエンドポイント: ネットワーク内の Apex One サーバの管理対象外エンドポイントを、企業のセキュリティガイドラインに準拠させることができます。

  詳細については、707 ページの「管理対象外のエンドポイントに関するセキュリティコンプライアンス」を参照してください。

手動で、または定期的に、Active Directory 構造を Apex One サーバと同期して、データの整合性を確保できます。

詳細については、62 ページの「Active Directory ドメインとのデータの同期」を参照してください。

Active Directory の Apex One との統合

手順

1. [管理] > [Active Directory] > [Active Directory 統合] に移動します。
2. [Active Directory ドメイン] で、Active Directory のドメイン名を指定します。
3. 指定された Active Directory ドメインとデータを同期する際に Apex One サーバで使用するアカウント情報を指定します。サーバがドメインに属していない場合には、アカウント情報が必要です。それ以外の場合、ドメインカウント情報は任意で使用します。これらのアカウント情報の有効期限が切れていないことを確認してください。有効期限が切れていると、サーバでデータを同期することはできません。

   a. [ドメインアカウント情報の指定] をクリックします。

   b. 開いたポップアップウィンドウに、ユーザ名とパスワードを入力します。ユーザ名は次のいずれかの形式で指定できます。

- ドメイン\ユーザ名
- ユーザ名@ドメイン

c. [保存]をクリックします。

4. さらにドメインを追加するには、(+) ボタンをクリックします。必要に応じて、追加したドメインのドメインアカウント情報を指定します。

5. ドメインを削除するには、(-) ボタンをクリックします。

6. ドメインアカウント情報を指定した場合は、暗号化の設定を指定します。セキュリティ保護の手段として、Apex One では、指定されたドメインアカウント情報を暗号化してデータベースに保存します。Apex One では、指定されたドメインのいずれかとデータを同期するときに、暗号化キーを使用してドメインアカウント情報を復号します。

   a. [ドメインアカウント情報の暗号化設定] セクションに移動します。

   b. 暗号化キーを 128 文字以内で入力します。

   c. 暗号化キーを保存するファイルを指定します。`.txt` などの一般的なファイル形式を選択できます。`C:¥AD_Encryption ¥EncryptionKey.txt` のように、ファイルのフルパスと名前を入力します。

警告!

ファイルが削除されたり、ファイルのパスが変更されたりした場合、Apex One では、指定されたすべてのドメインのデータを同期することはできなくなります。

---

7. 次のいずれかをクリックします。

   - 保存:設定のみを保存します。データの同期ではネットワークリソースに重い負荷がかかることがあるため、設定のみを保存して、重要な作業時間以外の時間帯に同期を実行するように選択できます。
   - 保存と同期:設定を保存して、データを Active Directory ドメインと同期します。

8. 定期的な同期スケジュールを設定します。詳細については、62 ページの「Active Directory ドメインとのデータの同期」を参照してください。

Active Directory ドメインとのデータの同期

Active Directory ドメインと定期的にデータを同期することで、Apex One エージェントツリー構造を最新の状態に維持して、管理対象外のエージェントに関するクエリを実行します。

Active Directory ドメインとのデータの手動同期

手順

1. [管理] > [Active Directory] > [Active Directory 統合] に移動します。
2. ドメインアカウント情報と暗号化設定が変更されていないことを確認します。
3. [保存と同期] をクリックします。

Active Directory ドメインとのデータの自動同期

手順

1. [管理] > [Active Directory] > [予約同期] に移動します。
2. [Active Directory の予約同期を有効にする] を選択します。
3. 同期スケジュールを指定します。

注意

毎日、毎週、毎月の同期の場合、Apex One が Active Directory と Apex One サーバを同期する期間を時間単位で指定します。

4. [保存] をクリックします。

Apex One エージェントツリー

Apex One エージェントツリーには、現在サーバで管理しているすべてのエージェントがドメイン別に表示されます。エージェントがドメインでグループ分けされているため、同じ設定をすべてのドメインメンバーに構成、管理、および適用できます。

エージェントの接続状態

セキュリティエージェントの接続状態は、Apex One サーバとセキュリティエージェントとの通信方法によって異なります。次の表に、セキュリティエージェントの各種の接続状態を示します。

表 2-8. エージェントの接続状態

接続状態	説明
オンライン	セキュリティエージェントが Apex One サーバに接続でき、以下の作業を目的とした双方向通信が可能です。 • ポリシー設定 • アップデート • 検索コマンド • 不審オブジェクトリストの同期 • サンプル送信 • ログ送信
オフライン	セキュリティエージェントから Apex One サーバまたはエッジリレーサーバへの接続が確立されていません。

接続状態	説明
スタンドアロン	セキュリティエージェントはサーバに接続できますが、通信に制限があります。スタンドアロンモードでの制限は次のとおりです。 • セキュリティエージェントはサーバからポリシー設定を受け取りません。 • セキュリティエージェントはサーバから検索コマンドを開始しません。 • セキュリティエージェントはサーバにログを送信しません。 Apex One サーバへの接続が確立されている場合、コンポーネントのアップデートを許可またはブロックする権限をスタンドアロンモードのエージェントに設定できます。 エンドユーザは、スタンドアロンモードのエージェントで検索やアップデートを手動で開始できます。
オフプレミス	セキュリティエージェントは企業のネットワーク外にあり、Apex One サーバに直接接続することはできません。ただし、エッジリレーサーバに接続して以下の作業を実行することができます。 • 不審オブジェクトリストの同期 • サンプル送信 • ログ送信 **注意** Apex One サーバはセキュリティエージェントに直接接続されていないため、エージェントツリーではオフプレミスエージェントの接続状態が「オフライン」と表示されます。

エージェントツリーのアイコン

Apex One エージェントツリーのアイコンは、エンドポイントの種類および Apex One が管理するセキュリティエージェントのステータスを視覚的に表しています。

表 2-9. Apex One エージェントツリーのアイコン

アイコン	説明
	ドメイン
	ルート
	アップデートエージェント
	従来型スキャンエージェント
	スマートスキャンを使用可能なセキュリティエージェント
	スマートスキャンを使用できないセキュリティエージェント
	スマートスキャンを使用可能なアップデートエージェント
	スマートスキャンを使用できないアップデートエージェント

エージェントツリーの検索

エージェントツリー ([エージェント] > [エージェント管理]) の上にある検索と表示の機能を使用して、Apex One で管理されるエンドポイントを特定します。

手順

- 管理対象エージェントを検索するには、[エンドポイントの検索] ボックスにエージェント名を入力します。

  該当するエージェントがエージェントツリーに表示されます。より詳細に検索オプションを指定するには、[詳細検索] をクリックします。

注意

IPv4 アドレスまたは IPv6 アドレスを使用するエンドポイントを特定するには、詳細検索機能を使用する必要があります。

詳細については、66 ページの「詳細検索オプション」を参照してください。

- ドメインを選択するとエージェントツリーの一覧が展開され、ドメインに属するエージェントとその関連情報が各列に表示されます。特定の列のみを表示するには、[エージェントツリー表示] で項目を選択します。
  - すべて表示: すべての列を表示
  - アップデート表示: すべてのコンポーネントとプログラムを表示
  - ウイルス対策表示: ウイルス対策コンポーネントを表示
  - スパイウェア対策表示: スパイウェア対策コンポーネントを表示
  - 情報漏えい対策オプション表示: エージェントの情報漏えい対策オプションモジュールのステータスを表示
  - ファイアウォール表示: ファイアウォールコンポーネントを表示
  - Smart Protection 表示: エージェント (従来型/スマートスキャン) と Trend Micro Smart Protection コンポーネントで使用されている検索方法を表示
  - アップデートエージェント表示: Apex One サーバによって管理されているすべてのアップデートエージェントに関する情報を表示
  - オフプレミスエージェント表示: エッジリレーサーバに報告するすべてのエージェントに関する情報を表示

詳細検索オプション

次の条件に基づいてエージェントを検索します。

セクション	説明
基本条件	IP アドレス、OS、ドメイン、MAC アドレス、検索方法、Web レピュテーションのステータスなど、エンドポイントの基本的な情報。 • IPv4 セグメントで検索するには、先頭オクテットで始まる IP アドレスの一部を指定する必要があります。IP アドレスに、指定した値が含まれるエンドポイントがすべて返されます。たとえば、10.5 と入力すると IP アドレスが 10.5.0.0〜10.5.255.255 の範囲のコンピュータがすべて返されます。 • IPv6 アドレスの範囲で検索するには、プレフィックスおよび長さを指定する必要があります。 • MAC アドレスによる検索には、16 進法範囲の MAC アドレス (例: 000A1B123C12) が必要です。
コンポーネントのバージョン	コンポーネント名の横にあるチェックボックスをオンにして、「より古い (指定値を含まない)」または「と同じか、より古い」を選択して条件を絞り込み、バージョン番号を入力します。初期設定では現在のバージョン番号が表示されます。
ステータス	エージェント設定

検索条件を指定してから [検索] をクリックします。条件を満たすエンドポイント名のリストがエージェントツリーに表示されます。

エージェントツリーに固有なタスク

エージェントツリーは、Web コンソールで特定の画面にアクセスすると表示されます。エージェントツリーの上部には、アクセスした画面に固有のメニュー項目が表示されます。これらのメニュー項目を使用して、エージェントの設定やエージェントタスクの起動など、特定のタスクを実行できます。タスクを実行するには、最初にタスクの実行対象を選択し、次にメニュー項目を選択します。

次の画面はエージェントツリーを示しています。

[エージェント管理] 画面

この画面を表示するには、[エージェント] > [エージェント管理] に移動します。

[エージェント管理] 画面で、一般的なエージェント設定を管理し、特定のエージェントのステータス情報 (ログオンユーザ、IP アドレス、接続状態など) を表示します。

次の表は、実行可能なタスクを示しています。

表 2-10. [エージェント管理]のタスク

メニューボタン	タスク
ステータス	詳細なエージェント情報を表示します。詳細については、693 ページの「セキュリティエージェントの情報の表示」を参照してください。
タスク	• エージェントエンドポイントで ScanNow を実行します。詳細については、296 ページの「ScanNow の開始」を参照してください。 • エージェントをアンインストールします。詳細については、200 ページの「Web コンソールからのセキュリティエージェントのアンインストール」を参照してください。 • 検出された不審ファイルを復元します。詳細については、316 ページの「隔離ファイルの復元」を参照してください。 • スパイウェア/グレーウェアコンポーネントを復元します。詳細については、325 ページの「スパイウェア/グレーウェアの復元」を参照してください。

設定	• 検索設定を行います。詳細については、次の項目を参照してください。
	  • 279 ページの「検索方法の種類」
	  • 288 ページの「手動検索」
	  • 285 ページの「リアルタイム検索」
	  • 291 ページの「予約検索」
	  • 293 ページの「ScanNow」
	• Web レピュテーション設定を行います。詳細については、517 ページの「Web レピュテーションポリシー」を参照してください。
	• 機械学習型検索の設定を行います。詳細については、393 ページの「機械学習型検索の設定」を参照してください。

メニューボタン	タスク
	• 不審接続監視設定を行います。詳細については、397 ページの「不審接続監視の設定」を参照してください。 • 挙動監視の設定を行います。詳細については、408 ページの「挙動監視」を参照してください。 • デバイスコントロール設定を行います。詳細については、432 ページの「デバイスコントロール」を参照してください。 • 情報漏えい対策のポリシーを設定します。詳細については、496 ページの「情報漏えい対策のポリシー設定」を参照してください。 • サンプル送信設定を行います。詳細については、400 ページの「サンプル送信の設定」を参照してください。 • エージェントをアップデートエージェントとして割り当てます。詳細については、259 ページの「アップデートエージェント設定」を参照してください。 • エージェントの権限とその他の設定を行います。詳細については、729 ページの「エージェントの権限とその他の設定」を参照してください。 • セキュリティエージェントサービスを有効または無効にします。詳細については、645 ページの「セキュリティエージェントサービス」を参照してください。 • スパイウェア/グレーウェアの承認済みリストを設定します。詳細については、323 ページの「スパイウェア/グレーウェアの承認済みリスト」を参照してください。 • 信頼済みプログラムリストを設定します。詳細については、327 ページの「信頼済みプログラムリストの設定」を参照してください。 • エージェント設定をインポートおよびエクスポートします。詳細については、693 ページの「エージェント設定のインポートとエクスポート」を参照してください。
ログ	次のログを表示します。 • ウイルス/不正プログラムログ (詳細については、362 ページの「ウイルス/不正プログラムログの表示」を参照) • スパイウェア/グレーウェアログ (詳細については、370 ページの「スパイウェア/グレーウェアログの表示」を参照)

メニューボタン	タスク
	• ファイアウォールログ (詳細については、564 ページの「ファイアウォールログ」を参照) • Web レピュテーションログ (詳細については、533 ページの「Web からの脅威のログ」を参照) • 不審接続監視ログ (詳細については、404 ページの「不審接続監視ログの表示」を参照) • 不審ファイルログ (詳細については、375 ページの「不審ファイルログの表示」を参照) • C&C コールバックログ (詳細については、534 ページの「C&C コールバックログの表示」を参照) • 挙動監視ログ (詳細については、427 ページの「挙動監視ログ」を参照) • 機械学習型検索ログ (詳細については、401 ページの「機械学習型検索ログの表示」を参照) • デバイスコントロールログ (詳細については、448 ページの「デバイスコントロールログ」を参照) • 情報漏えい対策ログ (詳細については、505 ページの「情報漏えい対策ログ」を参照) • 検索ログ (詳細については、376 ページの「検索ログの表示」を参照) ログを削除します。詳細については、616 ページの「ログ管理」を参照してください。
エージェントツリーの管理	エージェントツリーを管理します。詳細については、79 ページの「エージェントのグループ設定のタスク」を参照してください。
エクスポート	エージェントのリストをカンマ区切り形式 (.csv) のファイルにエクスポートします。

大規模感染予防サービス 画面

この画面を表示するには、[エージェント] > [大規模感染予防サービス] に移動します。

大規模感染予防サービス 画面で、大規模感染予防の設定を行ってアクティベートします。詳細については、381 ページの「セキュリティリスクの大規模感染予防の設定」を参照してください。

[エージェントの選択] 画面

この画面を表示するには、[アップデート] > [エージェント] > [手動アップデート] に移動します。[エージェントを手動で選択] を選択し、[選択] をクリックします。

[エージェントの選択] 画面で、手動アップデートを開始します。詳細については、249 ページの「セキュリティエージェントの手動アップデート」を参照してください。

[ロールバック] 画面

この画面を表示するには、[アップデート] > [ロールバック] に移動します。[サーバと同期] をクリックします。

[ロールバック] 画面でエージェントコンポーネントをロールバックします。詳細については、257 ページの「セキュリティエージェントコンポーネントのロールバック」を参照してください。

セキュリティリスクログ 画面

この画面を表示するには、[ログ] > [エージェント] > [セキュリティリスク] に移動します。

セキュリティリスクログ 画面で、ログを表示および管理します。

次のタスクを実行します。

1. エージェントがサーバに送信したログを表示します。詳細については、以下のページを参照してください。
   - 362 ページの「ウイルス/不正プログラムログの表示」
   - 370 ページの「スパイウェア/グレーウェアログの表示」

- 564 ページの「ファイアウォールログの表示」
- 533 ページの「Web レピュテーションログの表示」
- 404 ページの「不審接続監視ログの表示」
- 375 ページの「不審ファイルログの表示」
- 534 ページの「C&C コールバックログの表示」
- 428 ページの「挙動監視ログの表示」
- 401 ページの「機械学習型検索ログの表示」
- 448 ページの「デバイスコントロールログの表示」
- 506 ページの「情報漏えい対策ログの表示」
- 376 ページの「検索ログの表示」

2. ログを削除します。詳細については、616 ページの「ログ管理」を参照してください。

Apex One ドメイン

Apex One のドメインは、同じ設定を共有し、同じタスクを実行するエージェントのグループです。エージェントをドメインにグループ化することで、すべてのドメインメンバーに同じ設定を構成、管理、および適用できます。

エージェントのグループ設定の詳細については、72 ページの「エージェントのグループ設定」を参照してください。

エージェントのグループ設定

エージェントのグループ設定を使用して、Apex One エージェントツリー上にドメインを手動で、または自動的に作成して管理します。

セキュリティエージェントをグループ化するには、次の 2 種類の方法があります。

表 2-11. エージェントのグループ設定方法

方法	エージェントのグループ設定	説明
手動	• NetBIOS ドメイン • Active Directory ドメイン • DNS ドメイン	エージェントグループの手動設定では、新しくインストールしたエージェントを追加するドメインを定義します。エージェントがエージェントツリーに表示されると、別のドメインや別の Apex One サーバに移動できます。 また、エージェントグループの手動設定では、エージェントツリー内のドメインの作成、管理、および削除も実行できます。 詳細については、73 ページの「手動によるエージェントのグループ設定」を参照してください。
自動	カスタムエージェントグループ	エージェントグループの自動設定では、ルールを使用してエージェントツリー内のエージェントを並べ替えします。ルールを定義すると、エージェントツリーにアクセスしてエージェントを手動で並べ替えたり、特定イベントの発生時に Apex One で自動的に並べ替えたりできます。 詳細については、74 ページの「エージェントの自動グループ設定」を参照してください。

手動によるエージェントのグループ設定

この設定は、エージェントの新規インストール時にのみ使用されます。インストール先のエンドポイントが属するネットワークドメインがインストールプログラムで確認され、エージェントツリーにすでに存在するドメインの場合は、エンドポイント上のエージェントがそのドメインの下に追加されてそのドメインの設定が適用されます。存在しないドメインの場合、エージェントツリーにそのドメインが追加されてその下にエージェントが追加され、ドメインおよびエージェントにルート設定が適用されます。

エージェントグループの手動設定

手順

1. [エージェント] > [エージェントのグループ設定] に移動します。
2. エージェントのグループ設定方法を指定します。
   - NetBIOS ドメイン
   - Active Directory ドメイン
   - DNS ドメイン
3. [保存]をクリックします。

次に進む前に

ドメインおよびドメイン内にグループ設定したエージェントを管理するには、次のタスクを実行します。

- ドメインの追加
- ドメインまたはエージェントの削除
- ドメイン名の変更
- 別のドメインへの単一エージェントの移動

詳細については、79 ページの「エージェントのグループ設定のタスク」を参照してください。

エージェントの自動グループ設定

エージェントの自動グループ設定では、IP アドレスまたは Active Directory ドメインによって定義されるルールが使用されます。あるルールで IP アドレスまたは IP アドレス範囲が定義されている場合、Apex One サーバは一致する IP アドレスのエージェントをグループ化し、エージェントツリー内の特定のドメインに追加します。同様に、ルールに 1 つ以上の Active Directory ドメインが定義されている場合、Apex One サーバでは、特定の Active Directory ドメインに属するエージェントをグループ化し、エージェントツリー内の特定のドメインに追加します。

エージェントに同時に適用できるルールは 1 つのみです。エージェントが複数のルールの条件を満たす場合に最も優先順位が高いルールが適用されるよう、ルールに優先順位を設定します。

エージェントの自動グループ設定

手順

1. [エージェント] > [エージェントのグループ設定]に移動します。
2. [エージェントのグループ設定] セクションに移動して、[既存のセキュリティエージェント用のカスタムエージェントグループを作成する] を選択します。
3. [エージェントの自動グループ設定] セクションに移動します。
4. ルールの作成を開始するには、[追加] をクリックしてから [Active Directory]、または [IP アドレス] を選択します。
   - [Active Directory] を選択した場合の設定の説明については、76 ページの「Active Directory ドメインによるエージェントのグループ設定ルールの定義」を参照してください。
   - [IP アドレス] を選択した場合の設定の説明については、77 ページの「IP アドレスによるエージェントのグループ設定ルールの定義」を参照してください。
5. 複数のルールを作成した場合は、次の手順でルールに優先順位を設定します。
   a. ルールを選択します。
   b. [グループの優先度] 列の矢印をクリックして、リスト内でルールを上または下に移動します。新しい位置を反映するためにルールの ID 番号が変更されます。
6. エージェントの並べ替え時にルールを使用するには、次の手順に従います。
   a. 使用するルールのチェックボックスをオンにします。

b. [ステータス] を [オン] に切り替えて、ルールを有効にします。

注意

ルールのチェックボックスがオフの場合や、ルールを無効化している場合、エージェントツリーでエージェントを並べ替えてもそのルールは使用されません。たとえば、新しいドメインにすべてのエージェントを移動するルールでも、そのエージェントは移動されず現在のドメインにとどまります。

7. [ドメインの予約作成] セクションで並べ替えのスケジュールを指定します。

   a. [ドメインの予約作成を有効にする] を選択します。

   b. [ドメインの予約作成] で、スケジュールを指定します。

8. 次のオプションから選択します。

   - 保存してドメインを作成:77 ページの「IP アドレスによるエージェントのグループ設定ルールの定義」の手順 7、または 76 ページの「Active Directory ドメインによるエージェントのグループ設定ルールの定義」の手順 7 で新しいドメインを指定した場合は、このオプションを選択します。
   - 保存:新しいドメインを指定していないか、エージェントの並べ替え実行時にのみ新しいドメインを作成する場合は、このオプションを選択します。

注意

この手順を完了しても、エージェントの並べ替えは開始されません。

Active Directory ドメインによるエージェントのグループ設定ルールの定義

次の手順を実行する際は、事前に Active Directory 統合設定が完了していることを確認してください。詳細については、59 ページの「Active Directory 統合」を参照してください。

手順

1. [エージェント] > [エージェントのグループ設定] に移動します。
2. [エージェントのグループ設定] セクションに移動して、[既存のセキュリティエージェント用のカスタムエージェントグループを作成する] を選択します。
3. [エージェントの自動グループ設定] セクションに移動します。
4. [追加] をクリックして、[Active Directory] を選択します。

   新しい画面が表示されます。
5. [グループ設定を有効にする] を選択します。
6. ルールの名前を指定します。
7. [Active Directory ソース] で、Active Directory ドメイン、またはサブドメインを選択します。
8. [エージェントツリー] で、Active Directory ドメインのマップ先となる既存の Apex One ドメインを選択します。適切な Apex One ドメインが存在しない場合は、次の手順を実行します。
   a. 特定の Apex One ドメインにマウスを重ね、[ドメインの追加] アイコン (+) をクリックします。
   b. 表示されたテキストボックスにドメイン名を入力します。
   c. テキストボックスの横にあるチェックマークをクリックします。新しいドメインが追加され、自動的に選択されます。
9. (オプション) [Active Directory の構造をエージェントツリーに複製します] を選択します。このオプションによって、選択した Active Directory ドメインの階層が選択した Apex One ドメインに複製されます。
10. [保存]をクリックします。

IP アドレスによるエージェントのグループ設定ルールの定義

ネットワーク IP アドレスを使用してカスタムエージェントグループを作成し、Apex One エージェントツリーでエージェントを並べ替えます。この機能

により、管理者は、エージェントを Apex One サーバに登録する前に Apex One エージェントツリー構造を編成できます。

手順

1. [エージェント] > [エージェントのグループ設定]に移動します。
2. [エージェントのグループ設定] セクションに移動して、[既存のセキュリティエージェント用のカスタムエージェントグループを作成する] を選択します。
3. [エージェントの自動グループ設定] セクションに移動します。
4. [追加] をクリックして、[IP アドレス] を選択します。

   新しい画面が表示されます。
5. [グループ設定を有効にする] を選択します。
6. グループ設定の名前を指定します。
7. 次のいずれかを指定します。
   - 個別の IPv4 アドレスまたは IPv6 アドレス
   - IPv4 アドレス範囲
   - IPv6 プレフィックスおよび長さ

   注意

   デュアルスタックエージェントの IPv4 および IPv6 アドレスが異なる 2 つのエージェントグループに属している場合、そのエージェントは IPv6 グループになります。エージェントのホストコンピュータで IPv6 が無効になっている場合、このエージェントは IPv4 グループに移動します。
8. IP アドレスまたは IP アドレスの範囲のマップ先となる Apex One ドメインを選択します。ドメインが存在しない場合は、次の操作を実行します。
   a. エージェントツリーの任意の場所を選択し、[ドメインの追加] アイコンをクリックします。

b. 表示されたテキストボックスにドメインを入力します。

c. テキストボックスの横にあるチェックマークをクリックします。新しいドメインが追加され、自動的に選択されます。

9. [保存]をクリックします。

エージェントのグループ設定のタスク

ドメインにエージェントをグループ化する際、次のタスクを実行できます。

- ドメインの追加。詳細については、79 ページの「ドメインの追加」を参照してください。
- ドメインまたはエージェントの削除。詳細については、80 ページの「ドメインまたはエージェントの削除」を参照してください。
- ドメイン名の変更。詳細については、81 ページの「ドメイン名の変更」を参照してください。
- 別のドメインまたは別の Apex One サーバへの単一エージェントの移動。詳細については、81 ページの「別のドメインまたはサーバへのセキュリティエージェントの移動」を参照してください。

ドメインの追加

手順

1. [エージェント] > [エージェント管理] に移動します。
2. [エージェントツリーの管理] > [ドメインの追加] の順にクリックします。
3. 追加するドメインの名前を入力します。
4. [追加] をクリックします。

   エージェントツリーに新しいドメインが表示されます。
5. (オプション) サブドメインを作成します。

   a. 上位ドメインを選択します。

b. [エージェントツリーの管理] > [ドメインの追加] の順にクリックします。

c. サブドメイン名を入力します。

ドメインまたはエージェントの削除

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、次のいずれかを選択します。
   - 1 つ以上のドメイン
   - 特定のドメインに属する 1 つ、複数、またはすべてのエージェント
3. [エージェントツリーの管理] > [ドメイン/エージェントの削除] の順にクリックします。
4. 空のドメインを削除するには、[ドメイン/エージェントの削除] をクリックします。ドメインにエージェントが存在する場合に [ドメイン/エージェントの削除] をクリックすると、エージェントから Apex One サーバへの次回接続時にそのドメインが再作成され、そのドメイン下のすべてのエージェントがグループ化されます。ドメインを削除する前に次の操作を実行します。
   a. エージェントを別のドメインに移動します。エージェントを別のドメインに移動するには、それらを目的のドメインにドラッグ&ドロップします。
   b. すべてのエージェントを削除します。
5. 1 つのエージェントを削除するには、[ドメイン/エージェントの削除] をクリックします。

注意

エージェントツリーからエージェントを削除しても、エージェントエンドポイントからセキュリティエージェントが削除されることはありません。セキュリティエージェントでは、コンポーネントのアップデートなど、サーバに依存しないタスクを引き続き実行できます。ただし、サーバではそのエージェントが認識されなくなるため、設定や通知がエージェントに送信されなくなります。

ドメイン名の変更

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーでドメインを選択します。
3. [エージェントツリーの管理] > [ドメイン名の変更] の順にクリックします。
4. このドメインの新しい名前を入力します。
5. [拡張子変更] をクリックします。

   エージェントツリーに新しいドメイン名が表示されます。

別のドメインまたはサーバへのセキュリティエージェントの移動

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、1 つ、複数、またはすべてのエージェントを選択します。
3. [エージェントツリーの管理] > [エージェントの移動] の順にクリックします。
4. 別のドメインにエージェントを移動するには、次の手順を実行します。

- [選択したエージェントを別のドメインに移動する] を選択します。
- ドメインを選択します。
- (オプション) 新しいドメインの設定をエージェントに適用します。

ヒント

エージェントをドラッグ＆ドロップして、エージェントツリー内の別のドメインに移動することもできます。

5. 別のサーバにエージェントを移動するには、次の手順を実行します。
   - [選択したエージェントを別の Apex One サーバに移動する] を選択します。
   - サーバ名または IPv4/IPv6 アドレスと、HTTP または SSL (443) ポート番号を入力します。

     注意

     セキュリティエージェントを Apex One as a Service に移動する場合は、Apex Central コンソールにアクセスして Apex One as a Service サーバの情報を取得できます。[ディレクトリ] > [製品サーバ] に移動し、[サーバの種類] リストで [Apex One] を選択します。
6. [移動] をクリックします。

第 3 章

情報漏えい対策オプションの使用開始

この章では、情報漏えい対策オプションモジュールのインストールおよびアクティベート方法について説明します。

この章は次のトピックで構成されます。

情報漏えい対策オプションのインストール

情報漏えい対策オプションモジュールには次のような機能があります。

- 情報漏えい対策: デジタル資産が許可なく送信されるのを阻止します。
- デバイスコントロール: 外部デバイスへのアクセスの規制

注意

必要な機能を完備した Apex One には、USB ストレージデバイスなどのよく使用されるデバイスへのアクセスを規制するデバイスコントロール機能があります。デバイスコントロールは、情報漏えい対策オプションモジュールに含まれた機能であり、監視対象のデバイスの範囲を拡張します。監視対象デバイスのリストについては、432 ページの「デバイスコントロール」を参照してください。

情報漏えい対策とデバイスコントロールは、あらかじめ Apex One に組み込まれた機能ですが、ライセンスは別途必要です。Apex One サーバとこれらの機能は一緒にインストールされますが、使用したり、セキュリティエージェントに配信することはできません。情報漏えい対策オプションのインストールは、設定が完了しているトレンドマイクロのアップデートサーバまたはユーザ指定のアップデート元からファイルをダウンロードすることを意味します。このファイルの Apex One サーバへの組み込みを完了すれば、情報漏えい対策オプションライセンスをアクティベートしてその機能のすべてを有効にすることができます。インストールとアクティベーションは[プラグインマネージャ]から実行します。

情報漏えい対策オプションのインストール

手順

1. Apex One Web コンソールを開いて、メインメニューで [プラグイン] をクリックします。
2. [プラグインマネージャ]画面で、[Apex One 情報漏えい対策オプション] セクションに移動し、[ダウンロード] をクリックします。

   ダウンロードするファイルのサイズが、[ダウンロード] ボタンの横に表示されます。

プラグインマネージャによってダウンロードされたファイルは<サーバインストールフォルダ>¥PCCSRV¥Download¥Product に保存されます。

注意

プラグインマネージャでファイルがダウンロードできない場合は、24 時間後に自動的にダウンロードが再度行われます。Microsoft 管理コンソールから Apex One プラグインマネージャサービスを再起動することで、ファイルダウンロードを開始することもできます。

3. ダウンロードの進行状況を監視します。

   ダウンロード中に画面を切り替えることができます。

   ファイルのダウンロード中に問題が発生した場合は、Web コンソールでサーバアップデートログを確認します。メインメニューで、[ログ] > [サーバアップデート] の順にクリックします。

   プラグインマネージャによってファイルがダウンロードされると、情報漏えい対策オプションが新しい画面に表示されます。

注意

情報漏えい対策オプションが表示されない場合は、766 ページの「プラグインマネージャのトラブルシューティング」を確認してください。

4. 情報漏えい対策オプションを今すぐインストールするには、[インストール] をクリックします。後でインストールするには、次の手順を実行します。

   a. [後でインストール] をクリックします。

   b. [プラグインマネージャ] 画面を開きます。

   c. [Apex One 情報漏えい対策オプション] セクションに移動して、[インストール] をクリックします。

5. 使用許諾契約書を読み、その条項に同意できる場合は [同意する] をクリックしてその条項に同意すると、

   インストールが開始されます。

6. インストールの進捗状況を監視します。インストールが完了すると、情報漏えい対策オプションのバージョンが表示されます。

情報漏えい対策オプションライセンス

プラグインマネージャで、情報漏えい対策オプションライセンス情報の表示、アクティベート、およびサポート契約の更新を行います。

トレンドマイクロからアクティベーションコードを入手し、それを使用してライセンスをアクティベートします。

プラグインプログラムライセンスのアクティベート

手順

1. Apex One Web コンソールを開いて、メインメニューで [プラグイン] をクリックします。
2. [プラグインマネージャ] 画面で、プラグインプログラムのセクションに移動し、[プログラムの管理] をクリックします。

   [製品ライセンスの新しいアクティベーションコード] 画面が表示されます。
3. アクティベーションコードをテキストフィールドに入力するか、コピーして貼り付けます。
4. [保存] をクリックします。

   プラグインコンソールが表示されます。

ライセンス情報の表示と更新

手順

1. Apex One Web コンソールを開いて、メインメニューで [プラグイン] をクリックします。
2. [プラグインマネージャ] 画面で、プラグインプログラムのセクションに移動し、[プログラムの管理] をクリックします。
3. トレンドマイクロの Web サイトで現在のライセンスに関する情報を確認するには、[ライセンス情報の表示] をクリックします。
4. 表示された画面でライセンスに関する次の詳細を確認します。

オプション	説明
ステータス	[アクティベーション完了]、[アクティベーション未完了]、または [サポート契約終了] と表示されます。
バージョン	[製品版] または [体験版] バージョンのいずれかが表示されます。 **注意** 製品版と体験版の両方がアクティベートされている場合、「製品版」とのみ表示されます。
ライセンス有効期限	プラグインプログラムに複数のライセンスがある場合、最も遅い有効期限が表示されます。 たとえば、サポート契約の有効期限が 2010 年 12 月 31 日と 2010 年 6 月 30 日の場合は、2010 年 12 月 31 日が表示されます。
アクティベーションコード	アクティベーションコードが表示されます。
注意事項	現在のライセンスバージョンに応じて、更新猶予期間中 (製品版のみ) またはライセンスの有効期限が切れたときに、ライセンスの有効期限に関するメッセージが表示されます。

注意

プラグインプログラムの更新猶予期間については、トレンドマイクロの販売代理店にお問い合わせください。

5. 画面を最新のライセンス情報に更新するには、[ステータスをオンラインで確認] をクリックします。
6. [製品ライセンスの新しいアクティベーションコード] をクリックして、[製品ライセンスの新しいアクティベーションコード] 画面を開きます。

   詳細については、86 ページの「プラグインプログラムライセンスのアクティベート」を参照してください。

セキュリティエージェントへの情報漏えい対策オプションの配信

ライセンスをアクティベートしたら、情報漏えい対策オプションモジュールをセキュリティエージェントに配信します。配信後に、セキュリティエージェントで情報漏えい対策とデバイスコントロールの使用が開始されます。

重要

- Windows Server プラットフォームでは、初期設定で、ホストコンピュータの性能に影響を与えないようにこのモジュールが無効になっています。モジュールを有効にする場合は、システムの性能を継続的に監視し、性能の低下が確認された場合には必要な措置を取るようにしてください。

  モジュールは Web コンソールから有効または無効にすることができます。詳細については、645 ページの「セキュリティエージェントサービス」を参照してください。

- すでに、Trend Micro Data Loss Prevention ソフトウェアがエンドポイントに存在する場合は、Apex One によって情報漏えい対策オプションモジュールと置き換えられることはありません。

- エージェントがオンラインの場合は、ただちに情報漏えい対策オプションモジュールがインストールされます。エージェントがオフラインやスタンドアロンの場合は、Apex One サーバに再接続したときにモジュールがインストールされます。

- 情報漏えい対策ドライバのインストールを完了するには、ユーザがコンピュータを再起動する必要があります。事前に、再起動のことをユーザに通知しておいてください。

- 配信問題の解決を容易にするためにデバッグロギングを有効にすることをお勧めします。詳細については、511 ページの「情報漏えい対策オプションモジュールのデバッグログの有効化」を参照してください。

セキュリティエージェントへの情報漏えい対策オプションモジュールの配信

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで実行可能な操作は次のとおりです。
   - 既存のエージェントと今後追加されるエージェントのすべてにモジュールを配信するには、ルートドメインアイコン () をクリックします。

- 特定のドメインに属している既存のエージェントと将来のエージェントのすべてにモジュールを配信するには、そのドメインを選択します。
- 特定のエージェントにのみモジュールを配信するには、そのエージェントを選択します。

3. モジュールの配信には次の 2 つの方法があります。
   - [設定] > [情報漏えい対策設定] の順にクリックします。
   - [設定] > [デバイスコントロール設定] の順にクリックします。

   注意

   [設定] > [情報漏えい対策設定] から情報漏えい対策オプションモジュールが正常に配信された場合は、情報漏えい対策のドライバがインストールされます。ドライバが正常にインストールされると、インストールを完了するにはエンドポイントの再起動が必要であることを伝えるメッセージが表示されます。

   メッセージが表示されない場合は、ドライバのインストール中に問題が発生した可能性があります。デバッグロギングを有効にしていた場合は、デバッグログでドライバインストール問題の詳細を確認してください。

4. モジュールがインストールされなかったエージェントの数を示すメッセージが表示されます。[OK] をクリックして配信を開始します。

   注意

   [キャンセル] をクリックした場合 (または何らかの理由で 1 つ以上のエージェントにモジュールが配信されなかった場合) は、再度、[設定] > [情報漏えい対策設定] または [設定] > [デバイスコントロール設定] をクリックしたときに同じメッセージが表示されます。

   セキュリティエージェントでサーバからのモジュールのダウンロードが開始されます。

5. モジュールがエージェントに配信されたかどうかを確認します。
   a. エージェントツリーで、ドメインを選択します。

b. エージェントツリー表示で、[情報漏えい対策オプション表示] または [すべて表示] を選択します。

c. [情報漏えい対策オプションステータス] 列を確認します。配信ステータスは、次のいずれかになります。

- 実行中: モジュールが正常に配信され、その機能が有効になっています。
- 再起動が必要です: ユーザがコンピュータを再起動していないため、情報漏えい対策のドライバがインストールされていません。ドライバがインストールされなければ、情報漏えい対策は機能しません。
- 中止されました: モジュール用のサービスが開始されていないか、対象エンドポイントが正常にシャットダウンされました。情報漏えい対策オプションサービスを開始するには、[エージェント] > [エージェント管理]、[設定] > [追加サービス設定] に移動して、情報漏えい対策オプションサービスを有効にします。
- インストールできません: エージェントへのモジュール配信中に問題が発生しました。エージェントツリーからモジュールを配信し直す必要があります。
- インストールできません (情報漏えい対策はすでに存在します): Trend Micro Data Loss Prevention ソフトウェアがすでにエンドポイントに存在します。Apex One によって情報漏えい対策オプションモジュールに置き換えられることはありません。
- インストールされていません: モジュールがエージェントに配信されていません。このステータスは、モジュールをエージェントに配信しないように選択された場合、または、配信中のエージェントの状態がオフラインかスタンドアロンの場合に表示されます。

フォレンジックスフォルダと情報漏えい対策データベース

情報漏えい対策イベントが発生すると、イベントの詳細が特定のフォレンジックスデータベースにログとして記録されます。また、イベントを実行した機密データのコピーを含むファイルが作成されて暗号化され、検証用および機密データの完全性を確保するためにハッシュ値が生成されます。Apex One は、暗号化されたフォレンジックスファイルをエージェントコンピュータ上に作成した後、それらのファイルをサーバの特定の場所にアップロードします。

重要

- 暗号化されたフォレンジックスファイルには、非常に機密性の高いデータが含まれているため、管理者はこれらのファイルへのアクセスを付与する際には十分に注意する必要があります。
- Apex One は Apex Central と統合されているため、DLP Incident Reviewer または DLP Compliance Officer の役割を持つ Apex Central ユーザには、暗号化されたファイル内のデータへのアクセス権が付与されます。情報漏えい対策の役割と Apex Central でのフォレンジックスファイルデータへのアクセスの詳細については、Control Manager または Apex Central の管理者ガイドを参照してください。

フォレンジックスフォルダおよびデータベースの設定変更

管理者は、フォレンジックスフォルダの場所と削除スケジュール、およびエージェントからアップロードされるファイルの最大サイズを Apex One の INI ファイルを変更することによって変更できます。

警告!

情報漏えい対策イベントをログに記録した後でフォレンジックスフォルダの場所を変更すると、データベースのデータと既存のフォレンジックスファイルの場所との関連付けが分断される原因となります。フォレンジックスフォルダの場所を変更した後に、既存のフォレンジックスファイルを手動で新しいフォレンジックスフォルダに移動することをお勧めします。

次の表は、Apex One サーバにある<サーバインストールフォルダ>¥PCCSRV¥Private¥ofcserver.ini ファイルで使用可能なサーバ設定の概要を示しています。

表 3-1. PCCSRV¥Private¥ofcserver.ini でのフォレンジックスフォルダサーバの設定

目的	INI 設定	値
ユーザ指定のフォレンジックスフォルダを有効にする	[INI_IDLP_SECTION] EnableUserDefinedUploadFolder	0: 無効 (初期設定) 1: 有効
ユーザ指定のフォレンジックスフォルダを設定する	[INI_IDLP_SECTION] UserDefinedUploadFolder 注意 • 管理者は、情報漏えい対策にこの設定を適用する前に、EnableUserDefinedUploadFolder の設定を有効にする必要があります。 • フォレンジックスフォルダの初期設定の場所: <サーバインストールフォルダ>¥PCCSRV¥Private¥DLPForensicData • ユーザ指定のフォレンジックスフォルダは、サーバコンピュータ上の物理ドライブ (内部または外部) になければなりません。Apex One は、ネットワークドライブのマッピングはサポートしていません。	初期設定値:<この値はカスタマー定義のフォルダパスに置き換えてください。 例:C:¥VolumeData¥OfficeScanDlpForensicData> ユーザ指定値:サーバコンピュータ上のドライブの物理的な場所でなければなりません。
フォレンジックスデータファイルの削除を有効にする	[INI_IDLP_SECTION] ForensicDataPurgeEnable	0: 無効 1: 有効 (初期設定)

目的	INI 設定	値
フォレンジックスデータファイルの削除チェック間隔を設定する	[INI_IDLP_SECTION] ForensicDataPurgeCheckFrequency **注意** ・ 管理者は、Apex One でこの設定を適用する前に、ForensicDataPurgeEnable の設定を有効にする必要があります。 ・ Apex One は、ForensicDataExpiredPeriodInDays で指定された有効期限を過ぎたデータファイルのみを削除します。	1: 月次、毎月 1 日の 00:00 時 2: 週次 (初期設定)、毎週日曜日の 00:00 時 3: 日次、毎日 00:00 時 4: 毎時、毎時 00 分
フォレンジックスデータファイルをサーバに保存する期間を設定する	[INI_IDLP_SECTION] ForensicDataExpiredPeriodInDays	初期設定値 (日数): 180 最小値: 1 最大値: 3650
フォレンジックスファイルのディスク容量チェック間隔を設定する	[INI_SERVER_DISK_THRESHOLD] MonitorFrequencyInSecond **注意** フォレンジックスデータフォルダの利用可能なディスク容量が、InformUploadOnDiskFreeSpaceInGb の設定で指定された値より小さくなると、Apex One は Web コンソールでイベントログを記録します。	初期設定値 (秒数): 5

目的	INI 設定	値
フォレンジックスファイルのディスク容量チェックのアップロード頻度を設定する	[INI_SERVER_DISK_THRESHOLD] IsapiCheckCountInRequest 注意 フォレンジックスデータフォルダの利用可能なディスク容量が、InformUploadOnDiskFreeSpaceInGb の設定で指定された値より小さくなると、Apex One は Web コンソールでイベントログを記録します。	初期設定値 (ファイル数): 200
ディスク空き容量不足通知を実行する最小ディスク容量を設定する	[INI_SERVER_DISK_THRESHOLD] InformUploadOnDiskFreeSpaceInGb 注意 フォレンジックスデータフォルダ内の利用可能なディスク容量が設定値より少なくなると、Apex One は Web コンソールにイベントログを記録します。	初期設定値 (GB): 10
エージェントからフォレンジックスデータファイルをアップロードするために必要な最小容量を設定する	[INI_SERVER_DISK_THRESHOLD] RejectUploadOnDiskFreeSpaceInGb 注意 フォレンジックスデータフォルダの利用可能なディスク容量が設定値より少なくなると、エージェントはフォレンジックスデータファイルをサーバにアップロードせず、Apex One は Web コンソールにイベントログを記録します。	初期設定値 (GB): 1

次の表は、Apex One サーバ上にある<サーバインストールフォルダ>¥PCCSRV¥ofcscan.ini ファイルで使用可能なセキュリティエージェントの設定の概要を示しています。

表 3-2. PCCSRV¥ofcscan.ini でのフォレンジックスファイルのエージェント設定

目的	INI 設定	値
フォレンジックスデータファイルのサーバへのアップロードを有効にする	UploadForensicDataEnable	0: 無効 1: 有効 (初期設定)
セキュリティエージェントがサーバにアップロードできるファイルの最大サイズを設定する	UploadForensicDataSizeLimitInMb **注意** セキュリティエージェントは、設定サイズよりも小さいファイルのみをサーバに送信します。	初期設定値 (MB): 10 最小値: 1 最大値: 20
フォレンジックスデータファイルをセキュリティエージェントに保存する期間を設定する	ForensicDataKeepDays **注意** セキュリティエージェントは、指定の有効期間を過ぎたフォレンジックスデータファイルを前日の削除時刻に基づいて 1 日 1 回削除します。	初期設定値 (日数): 180 最小値: 1 最大値: 3650
セキュリティエージェントがサーバとの接続をチェックする間隔を設定する	ForensicDataDelayUploadFrequenceInMinutes **注意** セキュリティエージェントは、フォレンジックスファイルをサーバに自動的にアップロードできない場合、指定された間隔でファイルのアップロードを試みます。	初期設定値 (分数): 5 最小値: 5 最大値: 60

フォレンジックスデータのバックアップの作成

企業のセキュリティポリシーに従って、フォレンジックスデータ情報の保存に必要な期間が大きく異なる場合があります。サーバ上のディスク容量を空

けるためには、フォレンジックスフォルダデータおよびフォレンジックスデータベースの手動バックアップを実行することをお勧めします。

手順

1. サーバのフォレンジックスデータフォルダの場所に移動します。
   - 初期設定の場所:<サーバインストールフォルダ>¥PCCSRV¥Private¥DLPForensicData
   - カスタマイズしたフォレンジックスフォルダの場所を探すには、93 ページのユーザ指定のフォレンジックスフォルダの場所の設定を参照してください。
2. フォルダを新しい場所にコピーします。
3. フォレンジックスデータのデータベースを手動でバックアップするには、<サーバインストールフォルダ>¥PCCSRV¥Private に移動します。
4. DLPForensicDataTracker.db ファイルを新しい場所にコピーします。

情報漏えい対策オプションのアンインストール

プラグインマネージャから情報漏えい対策オプションモジュールをアンインストールした場合には、次の処理が実行されます。

- 情報漏えい対策に関係する、すべての設定とログが Apex One サーバから削除されます。
- 情報漏えい対策オプションモジュールから提供されるすべてのデバイスコントロールの設定がサーバから削除されます。
- 情報漏えい対策オプションモジュールがエージェントから削除されます。情報漏えい対策オプションモジュールを完全に削除するには、エージェントエンドポイントを再起動する必要があります。
- エージェントに情報漏えい対策ポリシーが適用されなくなります。
- デバイスコントロールが、次のデバイスへのアクセスを監視しなくなります。

- Bluetooth アダプタ
- COM および LPT ポート
- IEEE 1394 インタフェース
- イメージングデバイス
- 赤外線デバイス
- モデム
- PCMCIA カード
- Print Screen キー
- ワイヤレス NIC

情報漏えい対策オプションモジュールはいつでも再インストールできます。再インストールしたら、有効なアクティベーションコードを使用してライセンスをアクティベートします。

プラグインマネージャからの情報漏えい対策オプションのアンインストール

手順

1. Apex One Web コンソールを開いて、メインメニューで [プラグイン] をクリックします。
2. [プラグインマネージャ]画面で、[Apex One 情報漏えい対策オプション] セクションに移動し、[アンインストール] をクリックします。
3. アンインストールの進行状況を監視します。アンインストール中は、進行状況を示す画面から別の画面に移動できます。
4. アンインストール後に [プラグインマネージャ] 画面を更新します。情報漏えい対策オプションが再インストール可能になります。

パート II

セキュリティエージェントの保護

第 4 章

Trend Micro Smart Protection の使用

この章では、Trend Micro Smart Protection ソリューションについて説明し、このソリューションを使用するために必要な環境の設定方法について示します。

この章は次のトピックで構成されます。

Trend Micro Smart Protection について

Trend Micro Smart Protection は、顧客をセキュリティリスクや Web の脅威から保護する目的で設計された、次世代のクラウド-クライアント型コンテンツセキュリティ インフラストラクチャです。クラウド上に統合されたメールレピュテーション、Web レピュテーション、およびファイルレピュテーションの各テクノロジおよび脅威データベースに軽量のエージェントを使用してアクセスすることで、ローカルソリューションとホステッドソリューションの両方を活用し、社内ネットワーク、自宅、外出先を問わず、ユーザを保護します。ネットワークにアクセスする製品、サービス、ユーザが増えるにつれて顧客への保護機能は自動的に更新および強化され、リアルタイムな相互監視保護システムが構築されていきます。

インターネットクラウドで提供されているレピュテーションテクノロジ、検索テクノロジ、および相関分析テクノロジを組み込むことで、Trend Micro Smart Protection ソリューションは、パターンファイルのダウンロードに依存していた従来の負担を軽減し、デスクトップのアップデートに伴う一般的な延期を解消します。

新規ソリューションの必要性

従来のファイルベースの脅威処理方法では、エンドポイントの保護に必要なパターン (定義) のほとんどが定期的に配信されます。パターンファイルは、トレンドマイクロからエージェントにバッチで配信されます。エージェントのウイルス/不正プログラム予防ソフトウェアが新しいアップデートを受信すると、新しいウイルス/不正プログラムのリスクに対する一連のパターン定義がメモリに再ロードされます。新しいウイルス/不正プログラムのリスクが発生した場合には、保護を継続するために、このパターンファイルをもう一度部分的または全体的にアップデートして、エージェントに再ロードする必要があります。

長い間に、出現する脅威の絶対数は大幅に増加してきました。脅威の量の増加は、近年、指数級数的な伸びを示しています。この増加のペースは今日の既知のセキュリティリスクの量を大きく上回り、今後は、このセキュリティリスクの量が新種のセキュリティリスクになると予想されます。セキュリティリスクの量は、サーバやワークステーションのパフォーマンス、ネットワーク帯域幅の使用率、また一般に、適切な保護を提供するまでの全体的な時間や「保護にかかる時間」に影響する可能性があります。

ユーザがウイルス/不正プログラムの量の脅威にも対抗できることを目指した新しい手法がトレンドマイクロによって開拓されています。この先駆的な技術で使用されるテクノロジとアーキテクチャには、ウイルス/不正プログラムのシグネチャやパターンファイルの保存をクラウドに移行するテクノロジが採用されています。ウイルス/不正プログラムのシグネチャの保存をクラウドに移行することにより、将来出現する量のセキュリティリスクからユーザをより強固に保護できます。

Trend Micro Smart Protection サービス

Trend Micro Smart Protection では、クラウドに保存された不正プログラム対策シグネチャ、Web レピュテーション、および脅威のデータベースが提供されます。

Trend Micro Smart Protection サービスの内容は次のとおりです。

- ファイルレピュテーションサービス:ファイルレピュテーションサービスは、これまでエージェントコンピュータに保存されていた大量の不正プログラム対策シグネチャを Trend Micro Smart Protection ソースに移行します。

  詳細については、104 ページの「ファイルレピュテーションサービス」を参照してください。

- Web レピュテーションサービス:Web レピュテーションサービスは、これまでトレンドマイクロのみでホストされていた URL レピュテーションデータの、ローカル Trend Micro Smart Protection ソースでのホストを可能にします。両方のテクノロジにより、パターンファイルのアップデートや URL の妥当性の確認で消費される帯域幅を減らすことができます。

  詳細については、104 ページの「Web レピュテーションサービス」を参照してください。

- スマートフィードバック:トレンドマイクロは、世界各国で使用されているトレンドマイクロ製品から情報を収集し、新しい各種の脅威を積極的に特定しています。

  詳細については、105 ページの「スマートフィードバック」を参照してください。

ファイルレピュテーションサービス

ファイルレピュテーションサービスは、インターネットクラウドに格納されている膨大なデータベースを照会して対象ファイルのレピュテーション (評価) を確認します。不正プログラム情報はクラウドに格納されているので、すべてのユーザがそれを使用できます。パフォーマンスに優れたコンテンツ配信ネットワークとローカルのキャッシュサーバによって、確認プロセスで発生する待ち時間は最小限に抑えられます。クラウド-エージェント型のアーキテクチャは、より迅速な保護を実現し、パターンファイル配信の負荷を解消することに加えて、エージェントの全般的なフットプリントを大幅に削減します。

ファイルレピュテーションサービスを使用するには、エージェントをスマートスキャンモードにする必要があります。このドキュメントでは、これらのエージェントをスマートスキャンエージェントと呼びます。スマートスキャンモードでない、ファイルレピュテーションサービスを使用しないエージェントは従来型スキャンエージェントと呼びます。Apex One 管理者は、すべてまたは一部のエージェントをスマートスキャンモードに設定できます。

Web レピュテーションサービス

世界最大規模のドメインレピュテーションデータベースであるトレンドマイクロの Web レピュテーションテクノロジは、Web サイトの経過日数、配置場所の変更履歴、および不正プログラムの挙動分析により検出された不審な活動の兆候などの要素に基づいてレピュテーションスコアを割り当てることにより、Web ドメインの信頼性を追跡します。サイトは継続的に検索され、感染サイトへのユーザアクセスがブロックされます。Web レピュテーション機能により、ユーザがアクセスするページが安全で、ユーザの個人情報を引き出すよう設計された不正プログラム、スパイウェア、およびフィッシング詐欺などの Web の脅威が存在しないことを確認できます。精度を向上させると同時に誤検出を少なくするため、トレンドマイクロの Web レピュテーションテクノロジでは、サイト全体を分類またはブロックするのではなく、サイト内の特定のページまたはリンクにレピュテーションスコアを割り当てています。これは、以前に正規サイトの一部分のみがハッキングされ、長期にわたってレピュテーションが動的に変化したことに対応する処理です。

Web レピュテーションポリシーの遵守対象となるセキュリティエージェントでは、Web レピュテーションサービスが使用されます。Apex One 管理者は、

すべてまたは一部のエージェントに Web レピュテーションポリシーを適用できます。

スマートフィードバック

トレンドマイクロスマートフィードバックは、トレンドマイクロのテクノロジおよび 24 時間体制の TrendLabs の運用によって、トレンドマイクロの製品間での継続的な情報交換を実現しています。ユーザの 1 回の定期的なレピュテーションチェックによって新しい脅威が特定されるたびに、トレンドマイクロの脅威に関するデータベースがすべて自動的にアップデートされ、これ以降ユーザで所定の脅威が発生することがないようブロックされます。

顧客およびパートナーの広範囲にわたる世界的なネットワークを通して収集された脅威に関する情報を継続的に処理することによって、トレンドマイクロは、最新の脅威に対して自動的なリアルタイムの保護を提供し、住民を保護するために地域で行われる自動化された自警組織と同様に、「団結」することによるセキュリティの強化を実現しています。脅威に関して収集される情報は、特定の通信のコンテンツではなく、送信元の評価に基づいています。

トレンドマイクロに送信される情報のサンプルを次に示します。

- ファイルのチェックサム
- アクセスされた Web サイト
- サイズやパスなどのファイル情報
- 実行可能ファイルの名前

プログラムへの参加は、Web コンソールからいつでも終了できます。

ヒント

ご使用のエンドポイントを保護するためにスマートフィードバックに参加することは必須ではありません。参加は任意であり、いつでも参加の取り消しができます。トレンドマイクロ製品のすべてのお客さまに対する全体的な保護の強化に役立つので、スマートフィードバックへの参加をお勧めします。

Trend Micro Smart Protection Network の詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

Trend Micro Smart Protection ソース

トレンドマイクロは、ファイルレピュテーションサービスと Web レピュテーションサービスを Apex One および Trend Micro Smart Protection ソースに配信します。

Trend Micro Smart Protection ソースは、ウイルス/不正プログラムパターン定義の大部分をホストすることによってファイルレピュテーションサービスを提供します。セキュリティエージェントは、それ以外の定義をホストします。自身のパターン定義でファイルの危険性を判定できない場合には、エージェントから Trend Micro Smart Protection ソースに検索クエリが送信されます。Trend Micro Smart Protection ソースは、識別情報を使用してリスクを判定します。

Trend Micro Smart Protection ソースは、これまでトレンドマイクロがホストするサーバを介してのみ利用可能であった Web レピュテーションデータをホストすることによって、Web レピュテーションサービスを提供します。エージェントから Trend Micro Smart Protection ソースに Web レピュテーションクエリが送信され、ユーザがアクセスしようとしている Web サイトの評価が確認されます。エージェントは、Web サイトのレピュテーションを、エンドポイントに適用される特定の Web レピュテーションポリシーに関連付けて、対象サイトへのアクセスを許可するかブロックするかを判定します。

エージェントが接続する Trend Micro Smart Protection ソースは、エージェントの位置によって異なります。エージェントは、Trend Micro Smart Protection Network と Smart Protection Server のいずれかに接続できます。

Trend Micro Smart Protection Network

Trend Micro Smart Protection Network は、顧客をセキュリティリスクや Web の脅威から保護する目的で設計された、次世代のクラウドクライアント型コンテンツセキュリティ基盤です。オンプレミスのソリューションとトレンドマイクロのホステッドソリューションの両方の機能を強化して、企業ネットワーク内、自宅、または外出先などどこでもユーザを保護します。Smart

Protection Network は、軽量エージェントを使用して、 独自のインターネットクラウドで提供されているメールレピュテーション、Web レピュテーション、およびファイルレピュテーションの相関分析テクノロジおよび脅威データベースにアクセスします。より多くの製品、サービス、およびユーザがネットワークにアクセスすれば、それだけ顧客の保護機能が自動的に更新および強化され、ユーザにとってのリアルタイムのネイバーフッドウォッチ (近隣監視活動) 保護サービスが形成されます。

Trend Micro Smart Protection Network の詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

Smart Protection Server

Smart Protection Server は、ローカルの企業ネットワークにアクセス可能なユーザ向けのものです。ローカルサーバは、効率を最適化するために、Trend Micro Smart Protection サービスを企業ネットワーク内で実行します。

次の 2 種類の Smart Protection Server があります。

- 統合 Smart Protection Server:Apex One セットアッププログラムには統合 Smart Protection Server が含まれており、Apex One サーバがインストールされているエンドポイントに統合 Smart Protection Server がインストールされます。インストールが終了したら、Web コンソールからこのサーバの設定を管理します。統合 Smart Protection Server は、Apex One の小規模な導入を目的としています。より大規模な導入には、スタンドアロンの Smart Protection Server が必要です。
- スタンドアロン Smart Protection Server:スタンドアロン Smart Protection Server は、VMware または Hyper-V サーバにインストールします。スタンドアロンサーバには個別の管理コンソールがあり、Apex One Web コンソールからは管理されません。

Trend Micro Smart Protection ソースの比較

次の表に、Trend Micro Smart Protection Network と Smart Protection Server の相違点を示します。

表 4-1. Trend Micro Smart Protection ソースの比較

比較基準	SMART PROTECTION SERVER	TREND MICRO SMART PROTECTION NETWORK
使用可否	内部エージェント、つまり Web コンソールで指定した位置の条件に一致するエージェントで使用可能。	主に外部エージェント、つまり Web コンソールで指定した位置の条件に一致しないエージェントで使用可能。
目的	効率性を最適化するために、Trend Micro Smart Protection サービスを企業ネットワーク内に配置するよう設計されている。	企業ネットワークに直接アクセスできないエージェントに Trend Micro Smart Protection サービスを提供する、グローバル規模のインターネットベースインフラストラクチャ。
管理	Apex One 管理者がこれらの Trend Micro Smart Protection ソースをインストールおよび管理する。	トレンドマイクロがこのソースを管理する。
パターンアップデート元	トレンドマイクロのアップデートサーバ	トレンドマイクロのアップデートサーバ
エージェント接続プロトコル	HTTP および HTTPS	HTTPS

Trend Micro Smart Protection パターンファイル

Trend Micro Smart Protection パターンファイルは、ファイルレピュテーションサービスと Web レピュテーションサービスに使用されます。トレンドマイクロは、これらのパターンファイルをトレンドマイクロのアップデートサーバから配信します。

スマートスキャンエージェントパターンファイル

スマートスキャンエージェントパターンファイルは毎日アップデートされ、Apex One エージェントのアップデート元 (Apex One サーバまたはユーザ指定のアップデート元) によってダウンロードされます。その後、アップデート元からスマートスキャンエージェントにパターンが配信されます。

注意

スマートスキャンエージェントは、ファイルレピュテーションサービスを使用するよう管理者によって設定されているセキュリティエージェントです。ファイルレピュテーションサービスを使用しないエージェントは、「従来型スキャンエージェント」と呼ばれます。

スマートスキャンエージェントでは、セキュリティリスクの検索時にスマートスキャンエージェントパターンファイルが使用されます。このパターンでファイルのリスクを判定できない場合は、スマートスキャンパターンファイルと呼ばれる別のパターンが使用されます。

スマートスキャンパターンファイル

スマートスキャンパターンファイルは 1 時間ごとにアップデートされ、Trend Micro Smart Protection ソースによってダウンロードされます。スマートスキャンパターンファイルはスマートスキャンエージェントにはダウンロードされません。エージェントは、Trend Micro Smart Protection ソースに検索クエリを送信し、スマートスキャンパターンファイルに照らし合わせて潜在的脅威を検証します。

Web ブロックリスト

Web ブロックリストは、Trend Micro Smart Protection ソースによってダウンロードされます。Web レピュテーションポリシーの遵守対象となるセキュリティエージェントに Web ブロックリストがダウンロードされることはありません。

注意

管理者は、すべてまたは一部のエージェントに Web レピュテーションポリシーを適用できます。

Web レピュテーションポリシーの遵守対象となるエージェントでは、Trend Micro Smart Protection ソースに Web レピュテーションクエリを送信し、Web ブロックリストに照らし合わせて Web サイトの評価を検証します。エージェントは、Trend Micro Smart Protection ソースから受信したレピュ

テーションデータを、エンドポイントに適用される特定の Web レピュテーションポリシーに関連付け、このポリシーに基づいて対象サイトへのアクセスを許可するかブロックします。

Trend Micro Smart Protection パターンのアップデート処理

Trend Micro Smart Protection パターンのアップデートは、トレンドマイクロのアップデートサーバから配信されます。

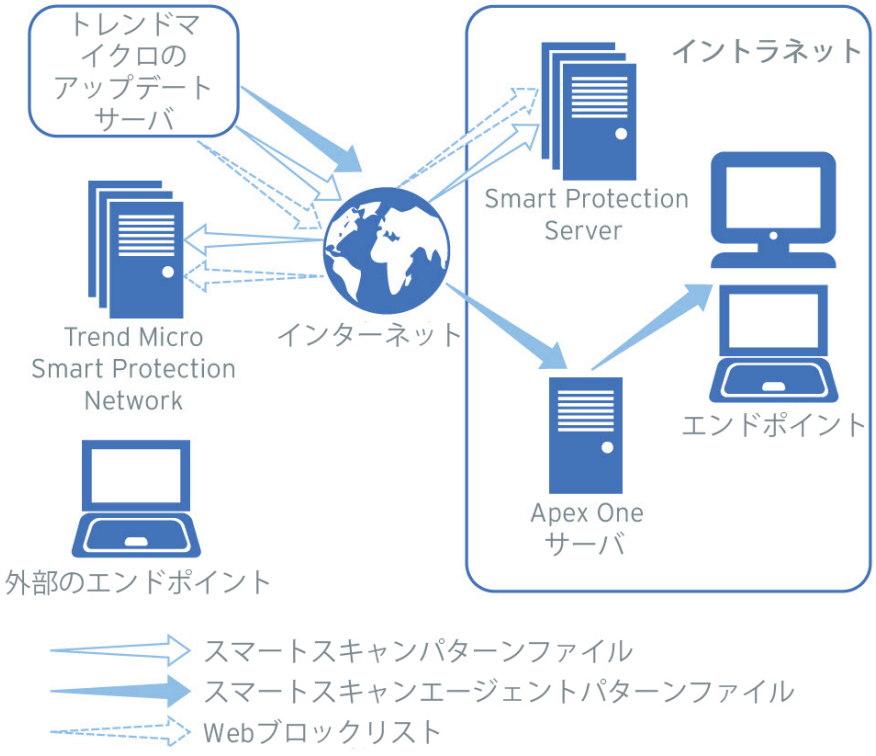


図 4-1. パターンファイルのアップデート処理

Trend Micro Smart Protection パターンの使用

セキュリティエージェントでは、スマートスキャンエージェントパターンファイルを使用してセキュリティリスクが検索され、スマートスキャンエージェントパターンファイルでファイルの危険性を判定できない場合にのみスマートスキャンパターンファイルにクエリが送信されます。ユーザが Web サイトにアクセスしようとすると、エージェントでは Web ブロックリストにクエリが実行されます。高度なフィルタリングテクノロジにより、エージェントではクエリの結果を「キャッシュ」できます。これにより、同じクエリを再度送信する必要がなくなります。

イントラネット上にあるエージェントは、Smart Protection Server に接続してスマートスキャンパターンファイルや Web ブロックリストにクエリを実行できます。Smart Protection Server に接続するにはネットワーク接続が必要です。設定されている Smart Protection Server が複数ある場合、管理者は、接続の優先順位を指定できます。

ヒント

複数の Smart Protection Server をインストールすることで、特定の Smart Protection Server への接続が不通になった場合にも保護を継続できます。

イントラネット上にないエージェントは、Trend Micro Smart Protection Network に接続してクエリを実行できます。Trend Micro Smart Protection Network に接続するにはインターネット接続が必要です。

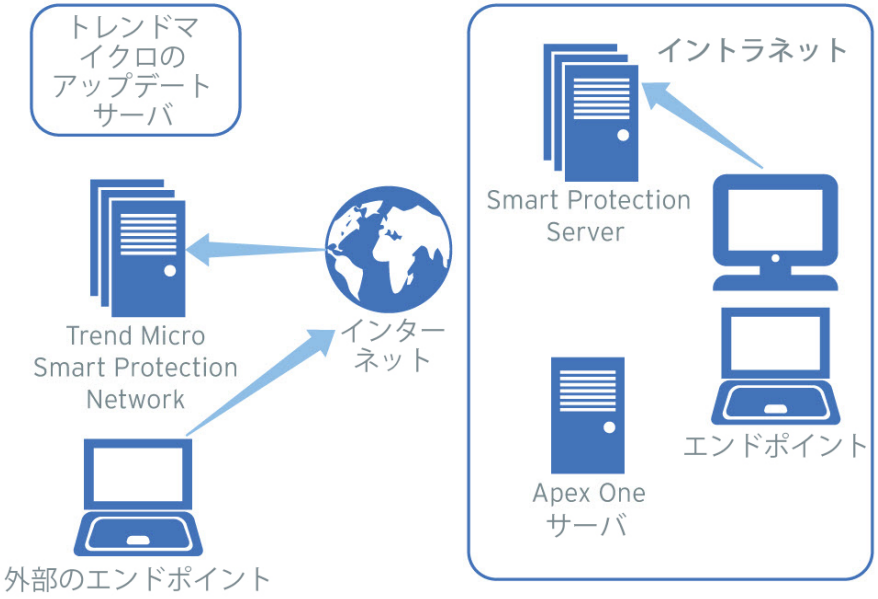


図 4-2. クエリの処理

ネットワークやインターネットにアクセスしないエージェントでも、スマートスキャンエージェントパターンファイルや以前のクエリ結果を含むキャッシュによって提供される保護を利用できます。この保護は、新しいクエリが必要になり、エージェントから繰り返しアクセスを試みたが、いずれの Trend Micro Smart Protection ソースにもアクセスできない場合には異なる動作を行います。この場合、エージェントは対象ファイルに検証フラグを付けて、一時的にファイルへのアクセスを許可します。Trend Micro Smart Protection ソースへの接続が回復すると、フラグが付けられているすべてのファイルが再検索されます。その後、脅威として確認されたファイルに、適切な検出時の処理が実行されます。

次の表は、エージェントの位置に基づいた保護の範囲についてまとめています。

表 4-2. 位置に基づいた保護動作

位置	パターンファイルとクエリ動作
イントラネットへのアクセス	• パターンファイル: エージェントは、Apex One サーバまたはユーザ指定のアップデート元からスマートスキャンエージェントパターンファイルをダウンロードします。 • ファイルレピュテーションおよび Web レピュテーションのクエリ:エージェントは Smart Protection Server に接続してクエリを実行します。
イントラネットに接続できないが、Trend Micro Smart Protection Network に接続可能	• パターンファイル:エージェントは、Apex One サーバまたはユーザ指定のアップデート元に接続できない限り、最新のスマートスキャンエージェントパターンファイルをダウンロードしません。 • ファイルレピュテーションおよび Web レピュテーションのクエリ:エージェントは Trend Micro Smart Protection Network に接続してクエリを実行します。
イントラネットにも Trend Micro Smart Protection Network にも接続不能	• パターンファイル:エージェントは、Apex One サーバまたはユーザ指定のアップデート元に接続できない限り、最新のスマートスキャンエージェントパターンファイルをダウンロードしません。 • ファイルレピュテーションおよび Web レピュテーションのクエリ:エージェントはクエリ結果を受信しないため、スマートスキャンエージェントパターンファイルや以前のクエリ結果を含むキャッシュに依存します。

Trend Micro Smart Protection サービスの設定

エージェントでファイルレピュテーションサービスと Web レピュテーションサービスを利用できるように、Trend Micro Smart Protection 環境を適切に設定しておく必要があります。次の項目を確認します。

- 114 ページの「Smart Protection Server のインストール」

- 119 ページの「統合 Smart Protection Server の管理」
- 123 ページの「Trend Micro Smart Protection ソースリスト」
- 132 ページの「エージェント接続のプロキシ設定」
- 132 ページの「エンドポイントの位置設定」
- 132 ページの「Trend Micro Network VirusWall のインストール」

Smart Protection Server のインストール

エージェント数が 1,000 以下の場合は、統合またはスタンドアロンの Smart Protection Server をインストールできます。エージェント数が 1,000 を超える場合は、スタンドアロンの Smart Protection Server をインストールしてください。

フェイルオーバーに対応するために、複数の Smart Protection Server をインストールすることをお勧めします。エージェントは、特定のサーバに接続できない場合、設定された別のサーバへの接続を試みます。

統合サーバと Apex One サーバは同じエンドポイント上で実行されるため、2 つのサーバのトラフィックがピークになるときには、エンドポイントのパフォーマンスが著しく低下する場合があります。スタンドアロン Smart Protection Server をプライマリ Trend Micro Smart Protection ソースとして使用し、統合サーバをバックアップとして使用することを検討してください。

スタンドアロン Smart Protection Server のインストール

スタンドアロン Smart Protection Server のインストールおよび管理の手順については、Smart Protection Server のインストールガイドを参照してください。

統合 Smart Protection Server のインストール

Apex One サーバのインストール時に統合サーバをインストールした場合は、次の操作を行ってください。

- 統合サーバを有効にして設定します。詳細については、119 ページの「統合 Smart Protection Server の管理」を参照してください。

- 統合サーバとセキュリティエージェントが同じサーバコンピュータ上に存在する場合は、Apex One ファイアウォールを無効にすることを検討してください。Apex One ファイアウォールはエージェントエンドポイントに対する使用を目的としているため、サーバ上で有効にするとパフォーマンスに影響を与える可能性があります。ファイアウォールを無効にする手順については、540 ページの「Apex One ファイアウォールの有効化/無効化」を参照してください。

注意

ファイアウォールを無効にした場合の影響を検討して、セキュリティ計画に従っていることを確認してください。

ヒント

115 ページの「統合 Smart Protection Server ツール」を使用して Apex One のインストールを完了したら、統合 Smart Protection Server をインストールします。

統合 Smart Protection Server ツール

トレンドマイクロの統合 Smart Protection ツールを使用すると、管理者は Apex One サーバのインストール完了後に、統合 Smart Protection Server をインストールまたはアンインストールできます。Apex One Web コンソールでは、Apex One サーバのインストールの完了後に管理者が統合 Smart Protection Server をインストールまたはアンインストールすることは許可されていません。

手順

1. コマンドプロンプトを開き、`ISPSInstaller.exe` のある<サーバインストールフォルダ>`¥PCCSRV\Admin\Utility\ISPSInstaller` ディレクトリに移動します。
2. 次のいずれかのコマンドを使用して、`ISPSInstaller.exe` を実行します。

表 4-3. インストーラオプション

コマンド	説明
`ISPSInstaller.exe /i`	初期設定のポートを使用して統合 Smart Protection Server をインストールします。 初期設定のポートの設定の詳細については、以下の表を参照してください。
`ISPSInstaller.exe /i /f:[port number] /s:[port number] /w:[port number]`	指定されたポートを使用して統合 Smart Protection Server をインストールします。 **注意** ポートを設定できるのは、Apache Web サーバを使用している場合だけです。 説明: • `/f:[port number]`: HTTP ファイルレピュテーションポート • `/s:[port number]`: HTTPS ファイルレピュテーションポート • `/w:[port number]`: Web レピュテーションポート **注意** ポートが指定されない場合は自動的に初期設定の値が割り当てられます。
`ISPSInstaller.exe /u`	統合 Smart Protection Server をアンインストールします。

表 4-4. 統合 Smart Protection Server のレピュテーションサービス用のポート

Web サーバおよび設定	ファイルレピュテーションサービス用のポート		Web レピュテーションサービス用の HTTP ポート
	HTTP	HTTPS (SSL)	
SSL が有効な IIS 既定 Web サイト	80	443 (設定不可)	80 (設定不可)
SSL が無効な IIS 既定 Web サイト	80	443 (設定不可)	80 (設定不可)
SSL が有効な IIS 仮想 Web サイト	8080	4343 (設定可能)	8080 (設定可能)
SSL が無効な IIS 仮想 Web サイト	8080	4343 (設定可能)	8080 (設定可能)

3. インストールが完了したら、Web コンソールを開いて、次を確認します。
   - Microsoft 管理コンソールを開き ([スタート] メニューで `services.msc` と入力)、Trend Micro Local Web Classification Server および Trend Micro Smart Scan Server が「開始」ステータスでリストされていることを確認します。
   - Windows タスクマネージャを開きます。[プロセス] タブで、`iCRCService.exe` および `LWCSService.exe` が実行中であることを確認します。
   - Web コンソールで、メニュー項目 [管理] > [Smart Protection] > [統合サーバ] が表示されることを確認します。

Smart Protection Server のベストプラクティス

Smart Protection Server のパフォーマンスを最適化するには、次の操作を行います。

- 手動検索と予約検索を同時に実行しないようにします。検索をグループに分けてタイミングをずらします。
- すべてのエージェントで ScanNow が同時に実行されないように設定します。

- ptngrowth.ini ファイルに変更を加えることで、低速のネットワーク接続 (約 512 Kbps) 用に Smart Protection Server をカスタマイズします。

ptngrowth.ini のスタンドアロンサーバ向けのカスタマイズ

手順

1. /var/tmcss/conf/にある ptngrowth.ini ファイルを開きます。
2. 次の推奨値を使用して、ptngrowth.ini ファイルを変更します。
   - `[COOLDOWN]`
   - `ENABLE=1`
   - `MAX_UPDATE_CONNECTION=1`
   - `UPDATE_WAIT_SECOND=360`
3. ptngrowth.ini ファイルを保存します。
4. コマンドラインインタフェース (CLI) から次のコマンドを入力して、lighttpd サービスを再起動します。
   - `service lighttpd restart`

ptngrowth.ini の統合サーバ向けのカスタマイズ

手順

1. <サーバインストールフォルダ>¥PCCSRV¥WSS¥にある ptngrowth.ini ファイルを開きます。
2. 次の推奨値を使用して、ptngrowth.ini ファイルを変更します。
   - `[COOLDOWN]`
   - `ENABLE=1`
   - `MAX_UPDATE_CONNECTION=1`

- `UPDATE_WAIT_SECOND=360`

3. `ptngrowth.ini` ファイルを保存します。
4. `Smart Protection Server` サービスを再起動します。

統合 Smart Protection Server の管理

統合 Smart Protection Server を管理するには、次のタスクを実行します。

- 統合サーバのファイルレピュテーションサービスと Web レピュテーションサービスを有効にする
- 統合サーバのアドレスを記録する
- 統合サーバのコンポーネントをアップデートする
- 統合サーバの承認済み URL リスト/URL ブロックリストを設定する

詳細については、122 ページの「統合 Smart Protection Server の設定」を参照してください。

統合サーバのファイルレピュテーションサービスと Web レピュテーションサービスを有効にする

エージェントから統合サーバに検索クエリと Web レピュテーションクエリを送信するには、ファイルレピュテーションサービスと Web レピュテーションサービスを有効にする必要があります。これらのサービスを有効にすると、統合サーバでトレンドマイクロのアップデートサーバからコンポーネントをアップデートできるようにもなります。

これらのサービスは、Apex One サーバのインストール時に統合サーバのインストールを選択することで自動的に有効になります。

これらのサービスを無効にする場合は、エージェントからクエリを送信できるスタンドアロン Smart Protection Server がインストールされていることを確認してください。

詳細については、122 ページの「統合 Smart Protection Server の設定」を参照してください。

統合サーバのアドレスを記録する

内部エージェント用の Trend Micro Smart Protection ソースリストを設定する際に、統合サーバのアドレスが必要になります。リストの詳細については、123 ページの「Trend Micro Smart Protection ソースリスト」を参照してください。

エージェントから統合サーバに検索クエリを送信する場合、エージェントではファイルレピュテーションサービスの 2 つのアドレスである HTTP アドレスと HTTPS アドレスのいずれかによってサーバが識別されます。HTTPS アドレス経由ではより安全な接続が可能ですが、HTTP 接続では消費される帯域幅が少なくなります。

エージェントから Web レピュテーションクエリを送信する場合、エージェントでは統合サーバの Web レピュテーションサービスアドレスによって統合サーバが識別されます。

ヒント

別の Apex One サーバによって管理されるエージェントも、この統合サーバに接続できます。他の Apex One サーバの Web コンソールで、統合サーバのアドレスを Trend Micro Smart Protection ソースリストに追加します。

詳細については、122 ページの「統合 Smart Protection Server の設定」を参照してください。

統合サーバのコンポーネントをアップデートする

統合サーバでは、次のコンポーネントがアップデートされます。

- スマートスキャンパターンファイル:セキュリティエージェントでは、統合サーバに検索クエリを送信し、スマートスキャンパターンファイルに照らし合わせて潜在的脅威を検証します。
- Web ブロックリスト:Web レピュテーションポリシーの遵守対象となるセキュリティエージェントでは、統合サーバに Web レピュテーションク

エリを送信し、Web ブロックリストに照らし合わせて Web サイトの評価を検証します。

これらのコンポーネントは手動でアップデートすることも、アップデートスケジュールを設定することもできます。統合サーバは、トレンドマイクロのアップデートサーバからコンポーネントをダウンロードします。

注意

IPv6 シングルスタック統合サーバでは、トレンドマイクロのアップデートサーバから直接アップデートすることはできません。統合サーバがトレンドマイクロのアップデートサーバに接続するには、DeleGate など、IP アドレスを変換できるデュアルスタックプロキシサーバが必要です。

詳細については、122 ページの「統合 Smart Protection Server の設定」を参照してください。

統合サーバの承認済み URL リスト/URL ブロックリストの設定

エージェントは、エージェント独自の承認済み URL リスト/URL ブロックリストを保持します。このリストは、Web レピュテーションポリシーの設定時に指定します (詳細については、517 ページの「Web レピュテーションポリシー」を参照してください)。エージェントのリストに含まれる URL は、すべて自動的に許可またはブロックされます。

統合サーバは、サーバ独自の承認済み URL リスト/URL ブロックリストを使用します。URL がエージェントのリストに含まれていない場合、エージェントから統合サーバに Web レピュテーションクエリが送信されます (統合サーバが Trend Micro Smart Protection ソースとして割り当てられている場合)。URL が統合サーバの承認済み URL リスト/URL ブロックリストで見つかると、統合サーバからエージェントにその URL を許可またはブロックする通知が送信されます。

注意

URL ブロックリストは、Web ブロックリストよりも優先されます。

URL を統合サーバの承認済みリスト/ブロックリストに追加するには、スタンドアロンの Smart Protection Server からリストをインポートします。URL を手動で追加することはできません。

詳細については、122 ページの「統合 Smart Protection Server の設定」を参照してください。

統合 Smart Protection Server の設定

手順

1. [管理] > [Smart Protection] > [統合サーバ] に移動します。
2. [ファイルレピュテーションサービスを有効にする] を選択します。
3. エージェントで統合サーバへの検索クエリの送信に使用するプロトコル (HTTP または HTTPS) を選択します。
4. [Web レピュテーションサービスを有効にする] を選択します。
5. [サーバアドレス] 列に表示される統合サーバのアドレスを記録します。
6. 統合サーバのコンポーネントをアップデートするには
   - スマートスキャンパターンファイルおよび Web ブロックリストの現在のバージョンを表示します。アップデートが入手可能な場合は、[今すぐアップデート] をクリックします。画面の上部にアップデートの結果が表示されます。
   - パターンを自動的にアップデートするには
     a. [予約アップデートを有効にする] を選択します。
     b. 1 時間ごとと 15 分ごとのいずれでアップデートするかを選択します。
     c. [ファイルレピュテーションサービス] からアップデート元を選択します。スマートスキャンパターンファイルがこのアップデート元からアップデートされるようになります。

d. [Web レピュテーションサービス] からアップデート元を選択します。Web ブロックリストがこのアップデート元からアップデートされるようになります。

注意

- アップデート元としてトレンドマイクロのアップデートサーバを選択する場合は、サーバがインターネットに接続されていることを確認し、プロキシサーバを使用している場合は、プロキシ設定を使用してインターネット接続が可能かどうかをテストしてください。詳細については、222 ページの「Apex One サーバアップデートのプロキシ」を参照してください。
- ユーザ指定のアップデート元を選択する場合は、適切な環境を設定して、このアップデート元のリソースをアップデートしてください。また、サーバコンピュータとこのアップデート元との接続が機能することも確認してください。アップデート元の設定について支援が必要な場合には、サポートセンターまでお問い合わせください。

---

7. 統合サーバの承認済みリスト/ブロックリストを設定するには
   a. [インポート] をクリックして、フォーマット済みの .csv ファイルから URL をリストに移行します。.csv ファイルは、スタンドアロンの Smart Protection Server から取得できます。
   b. 既存のリストがある場合は、[エクスポート] をクリックして、そのリストを .csv ファイルに保存します。
8. [保存]をクリックします。

Trend Micro Smart Protection ソースリスト

エージェントは、セキュリティリスクの検索時と Web サイトのレピュテーション判定時に Trend Micro Smart Protection ソースにクエリを送信します。

Trend Micro Smart Protection ソースに対する IPv6 のサポート

IPv6 シングルスタックエージェントからは、次のような IPv4 シングルスタックソースに直接クエリを送信することはできません。

- Trend Micro Smart Protection Network

同様に、IPv4 シングルスタックエージェントからは、IPv6 シングルスタックの Smart Protection Server にクエリを送信することはできません。

エージェントがこれらのソースに接続するには、DeleGate など、IP アドレスを変換できるデュアルスタックプロキシサーバが必要です。

Trend Micro Smart Protection ソースとエンドポイントの位置

エージェントが接続する Trend Micro Smart Protection ソースは、エージェントエンドポイントの位置によって異なります。

位置設定の指定方法については、640 ページの「エンドポイント (コンピュータ)の位置」を参照してください。

表 4-5. 位置による Trend Micro Smart Protection ソース

位置	TREND MICRO SMART PROTECTION ソース
外部	外部エージェントは、Trend Micro Smart Protection Network に検索クエリと Web レピュテーションクエリを送信します。

位置	TREND MICRO SMART PROTECTION ソース
内部	内部エージェントは、Smart Protection Server または Trend Micro Smart Protection Network に検索クエリと Web レピュテーションクエリを送信します。 Smart Protection Server をインストールした場合には、Web コンソールで Trend Micro Smart Protection ソースリストを設定します。内部エージェントは、クエリの実行が必要になった場合、このリストからサーバを選択します。エージェントが最初のサーバに接続できない場合は、別のサーバをリストから選択します。 ヒント スタンドアロンの Smart Protection Server をプライマリスキャンソースとして割り当てて、統合サーバをバックアップとして割り当てます。これにより、Apex One サーバと統合サーバをホストするエンドポイントへのトラフィックが削減されます。また、スタンドアロンサーバで、より多くのクエリ処理が可能になります。 Trend Micro Smart Protection ソースの標準リストまたはカスタムリストを設定できます。標準リストは、すべての内部エージェントで使用されます。カスタムリストでは、IP アドレスの範囲が定義されます。ある内部エージェントの IP アドレスが範囲内にある場合、そのエージェントはカスタムリストを使用します。

Trend Micro Smart Protection ソースの標準リストを設定する

手順

1. [管理] > [Smart Protection] > [Smart Protection ソース] に移動します。
2. [内部エージェント] タブをクリックします。
3. [標準リスト (すべての内部エージェント用のリスト) を使用する] を選択します。
4. [標準リスト] リンクをクリックします。

   新しい画面が表示されます。
5. [追加] をクリックします。

新しい画面が表示されます。

6. Smart Protection Server のホスト名または IPv4/IPv6 アドレスを指定します。IPv6 アドレスを指定する場合は、カッコ ( ) で囲んで指定します。

注意

Smart Protection Server に接続している IPv4 および IPv6 エージェントがある場合は、ホスト名を指定します。

---

7. [ファイルレピュテーションサービス] を選択します。エージェントは、HTTP または HTTPS プロトコルを使用して検索クエリを送信します。HTTPS はより安全な接続を提供しますが、HTTP は消費される帯域幅を抑えることができます。

   a. エージェントで HTTP を使用するよう指定するには、HTTP 要求用のサーバの待機ポートを入力します。エージェントで HTTPS を使用するよう指定するには、[SSL] を選択して、HTTPS 要求用のサーバの待機ポートを入力します。

   b. [接続テスト] をクリックして、サーバへの接続を確立できることを確認します。

ヒント

待機ポートはサーバアドレスの一部を形成します。サーバアドレスを取得するには、次の操作を実行します。

統合サーバの場合、Apex One Web コンソールを開き、[管理] > [Smart Protection] > [統合サーバ] に移動します。

スタンドアロンサーバの場合、スタンドアロンサーバのコンソールを開き、[概要] 画面に進みます。

---

8. [Web レピュテーションサービス] を選択します。エージェントは、HTTP プロトコルを使用して Web レピュテーションクエリを送信します。HTTPS はサポートされていません。

   a. HTTP 要求用のサーバの待機ポートを入力します。

   b. [接続テスト] をクリックして、サーバへの接続を確立できることを確認します。

9. [保存]をクリックします。

   画面が閉じます。

10. さらにサーバを追加するには、ここまでの手順を繰り返します。

11. 画面の上部で、[順序] または [ランダム] を選択します。

    - 順序: エージェントは、リストの表示順でサーバを選択します。[順序] を選択した場合は、[順序] 列の下の矢印を使用して、サーバをリストで上下に移動します。
    - ランダム: エージェントはサーバをランダムに選択します。

    ヒント

    統合 Smart Protection Server と Apex One サーバは同じエンドポイント上で実行されるため、2 つのサーバのトラフィックがピークになるときには、エンドポイントのパフォーマンスが著しく低下する場合があります。Apex One サーバへのトラフィックを減らすには、スタンドアロン Smart Protection Server をプライマリ Trend Micro Smart Protection ソースとして割り当てて、統合サーバをバックアップソースとして割り当てます。

    ---

12. 画面のその他のタスクを実行します。

    - 別のサーバからリストをエクスポートしている場合、この画面にインポートするときは、[インポート] をクリックして、`.dat` ファイルを選択します。リストが画面にロードされます。
    - リストを`.dat` ファイルにエクスポートするには、[エクスポート] をクリックし、[保存] をクリックします。
    - サーバのサービスステータスの表示を更新するには、[表示更新] をクリックします。
    - サーバ名をクリックして、次のいずれかを実行します。
      - サーバ情報を表示または編集します。
      - Web レピュテーションサービスまたはファイルレピュテーションサービスの完全なサーバアドレスを表示します。
    - Smart Protection Server のコンソールを開くには、[コンソールの起動] をクリックします。

- 統合 Smart Protection Server の場合は、サーバの設定画面が表示されます。
- スタンドアロンの Smart Protection Server、および別の Apex One サーバの統合 Smart Protection Server の場合は、コンソールのログオン画面が表示されます。

- エントリを削除するには、サーバのチェックボックスをオンにして、[削除] をクリックします。

13. [保存]をクリックします。

    画面が閉じます。

14. [すべてのエージェントに通知] をクリックします。

Trend Micro Smart Protection ソースのカスタムリストを設定する

手順

1. [管理] > [Smart Protection] > [Smart Protection ソース] に移動します。
2. [内部エージェント] タブをクリックします。
3. [エージェントの IP アドレスに基づいたカスタムリストを使用する] を選択します。
4. (オプション) [カスタムリスト上のすべてのサーバが使用不可の場合は標準リストを使用する] を選択します。

   ヒント

   カスタムソースが使用できなくなった場合にエージェントが Smart Protection ソースに接続できるように、この機能を有効にすることをお勧めします。

5. [追加] をクリックします。

   新しい画面が表示されます。

6. [IP 範囲] セクションで、IPv4 アドレス範囲と IPv6 アドレス範囲のいずれかまたは両方を指定します。

注意

IPv4 アドレスを持つエージェントは、IPv4 シングルスタックまたはデュアルスタックの Smart Protection Server に接続できます。IPv6 アドレスを持つエージェントは、IPv6 シングルスタックまたはデュアルスタックの Smart Protection Server に接続できます。IPv4 アドレスと IPv6 アドレスの両方を持つエージェントは、どの Smart Protection Server にも接続できます。

7. [プロキシ設定] セクションで、エージェントが Smart Protection Server への接続に使用するプロキシ設定を指定します。

   a. [エージェントと Smart Protection Server 間通信にプロキシサーバを使用する] を選択します。

   b. プロキシサーバの名前または IPv4/IPv6 アドレス、およびポート番号を指定します。

   c. プロキシサーバで認証が必要な場合は、ユーザ名とパスワードを入力します。

8. [Smart Protection Server のカスタムリスト] に、Smart Protection Server を追加します。

   a. Smart Protection Server のホスト名または IPv4/IPv6 アドレスを指定します。IPv6 アドレスを指定する場合は、カッコ ( ) で囲んで指定します。

注意

Smart Protection Server に接続している IPv4 および IPv6 エージェントがある場合は、ホスト名を指定します。

   b. [ファイルレピュテーションサービス] を選択します。エージェントは、HTTP または HTTPS プロトコルを使用して検索クエリを送信します。HTTPS はより安全な接続を提供しますが、HTTP は消費される帯域幅を抑えることができます。

i. エージェントで HTTP を使用するよう指定するには、HTTP 要求用のサーバの待機ポートを入力します。エージェントで HTTPS を使用するよう指定するには、[SSL] を選択して、HTTPS 要求用のサーバの待機ポートを入力します。

ii. [接続テスト] をクリックして、サーバへの接続を確立できることを確認します。

ヒント

待機ポートはサーバアドレスの一部を形成します。サーバアドレスを取得するには、次の操作を実行します。

統合サーバの場合、Apex One Web コンソールを開き、[管理] > [Smart Protection] > [統合サーバ] に移動します。

スタンドアロンサーバの場合、スタンドアロンサーバのコンソールを開き、[概要] 画面に進みます。

---

c. [Web レピュテーションサービス] を選択します。エージェントは、HTTP プロトコルを使用して Web レピュテーションクエリを送信します。HTTPS はサポートされていません。

i. HTTP 要求用のサーバの待機ポートを入力します。

ii. [接続テスト] をクリックして、サーバへの接続を確立できることを確認します。

d. [リストに追加] をクリックします。

e. さらにサーバを追加するには、ここまでの手順を繰り返します。

f. [順序] または [ランダム] を選択します。

- 順序: エージェントは、リストの表示順でサーバを選択します。[順序] を選択した場合は、[順序] 列の下の矢印を使用して、サーバをリストで上下に移動します。
- ランダム: エージェントはサーバをランダムに選択します。

ヒント

統合 Smart Protection Server と Apex One サーバは同じコンピュータ上で実行されるため、2 つのサーバのトラフィックがピークになるときには、コンピュータのパフォーマンスが著しく低下する場合があります。Apex One サーバへのトラフィックを減らすには、スタンドアロン Smart Protection Server をプライマリ Smart Protection ソースとして割り当てて、統合サーバをバックアップソースとして割り当てます。

g. 画面のその他のタスクを実行します。

- サーバのサービスステータスの表示を更新するには、[表示更新] をクリックします。
- Smart Protection Server のコンソールを開くには、[コンソールの起動] をクリックします。
  - 統合 Smart Protection Server の場合は、サーバの設定画面が表示されます。
  - スタンドアロンの Smart Protection Server、および別の Apex One サーバの統合 Smart Protection Server の場合は、コンソールのログオン画面が表示されます。
- エントリを削除するには、[削除] (削除) をクリックします。

9. [保存]をクリックします。

   画面が閉じます。追加したリストが [IP 範囲] 表の下に IP 範囲のリンクとして表示されます。

10. さらにカスタムリストを追加するには、手順 4～8 を繰り返します。

11. 画面のその他のタスクを実行します。

- リストを変更するには、対象の IP 範囲のリンクをクリックして、表示される画面で設定を変更します。
- リストを.dat ファイルにエクスポートするには、[エクスポート] をクリックし、[保存] をクリックします。

- 別のサーバからリストをエクスポートしている場合、この画面にインポートするときは、[インポート] をクリックして、.dat ファイルを選択します。リストが画面にロードされます。

12. [すべてのエージェントに通知] をクリックします。

エージェント接続のプロキシ設定

Trend Micro Smart Protection Network への接続にプロキシ認証が必要な場合には、認証用の資格情報を指定します。

Smart Protection Server への接続にエージェントが使用する内部プロキシ設定を指定します。

詳細については、687 ページの「セキュリティエージェントプロキシ設定」を参照してください。

エンドポイントの位置設定

Apex One の位置認識機能では、エージェントコンピュータの位置を識別し、エージェントが Trend Micro Smart Protection Network と Smart Protection Server のどちらに接続するかを判定します。これにより、エージェントはその位置に関係なく保護されます。

位置設定の指定方法については、640 ページの「エンドポイント (コンピュータ)の位置」を参照してください。

Trend Micro Network VirusWall のインストール

Trend Micro Network VirusWall Enforcer がインストールされている場合には、次の作業を実行してください。

- HotFix (Network VirusWall Enforcer 2500 用のビルド 1047、および Network VirusWall Enforcer 1200 用のビルド 1013) をインストールします。

- OPSWAT エンジンをバージョン 2.5.1017 にアップデートし、エージェントの検索方法が検出されるようにします。

Trend Micro Smart Protection サービスの使用

Trend Micro Smart Protection 環境を適切に設定したら、エージェントで、ファイルレピュテーションサービスと Web レピュテーションサービスを使用できます。スマートフィードバックの設定を開始することもできます。

注意

Trend Micro Smart Protection 環境を設定する手順については、113 ページの「Trend Micro Smart Protection サービスの設定」を参照してください。

ファイルレピュテーションサービスによる保護を利用するには、エージェントは「スマートスキャン」と呼ばれる検索方法を使用する必要があります。スマートスキャンの詳細およびエージェントでスマートスキャンを有効にする方法については、279 ページの「検索方法の種類」を参照してください。

セキュリティエージェントで Web レピュテーションサービスを使用できるようにするには、Web レピュテーションポリシーを設定します。詳細については、517 ページの「Web レピュテーションポリシー」を参照してください。

注意

検索方法および Web レピュテーションポリシーは細かく設定できます。要件に応じて、すべてのエージェントに適用する設定を指定することも、個々のエージェントやエージェントグループに適用する個別の設定を指定することもできます。

スマートフィードバックの設定手順については、636 ページの「スマートフィードバック」を参照してください。

第 5 章

セキュリティエージェントのインストール

この章では、Trend Micro Apex One のシステム要件およびセキュリティエージェントのインストール手順について説明します。

セキュリティエージェントのバージョンアップの詳細については、***インストールガイド***を参照してください。

この章は次のトピックで構成されます。

セキュリティエージェントの新規インストール

セキュリティエージェントは、Microsoft Windows プラットフォームを実行しているコンピュータにインストールできます。Apex One は、さまざまなサードパーティ製品と互換性があります。

システム要件および互換性のあるサードパーティ製品の完全なリストについては、次の Web サイトを参照してください。

http://www.go-tm.jp/corp/req

インストールの注意事項

セキュリティエージェントをインストールする前に、次の点を考慮してください。

表 5-1. セキュリティエージェントインストールの注意事項

注意事項	説明
Windows 機能のサポート	セキュリティエージェントの機能の中には、特定の Windows プラットフォームで使用できないものがあります。
IPv6 のサポート	セキュリティエージェントは、デュアルスタックエンドポイントまたは IPv6 シングルスタックエンドポイントにインストールできます。ただし、次の点に注意してください。 • セキュリティエージェントをインストールできる Windows OS の中には、Iv6 アドレスをサポートしていないものがあります。 • 一部のインストール方法には、セキュリティエージェントを正常にインストールするための特別な要件があります。
セキュリティエージェントの IP アドレス	IPv4 アドレスと IPv6 アドレスの両方を持つセキュリティエージェントについては、セキュリティエージェントをサーバに登録する際に使用する IP アドレスを選択できます。

注意事項	説明
除外リスト	次の機能に対して除外リストを正しく設定します。 • 挙動監視: セキュリティエージェントが重要なエンドポイントアプリケーションをブロックしないように、承認済みプログラムリストにそれらのアプリケーションを追加します。 詳細については、415 ページの「挙動監視除外リスト」を参照してください。 • Web レピュテーション: 安全と考えられる Web サイトへのアクセスをセキュリティエージェントがブロックしないように、承認済み URL リストに Web サイトを追加します。 詳細については、517 ページの「Web レピュテーションポリシー」を参照してください。

セキュリティエージェントの機能

エンドポイントで使用できるセキュリティエージェントの機能は、OS によって異なります。

表 5-2. サーバプラットフォーム上のセキュリティエージェントの機能

機能	Windows OS			
	Windows Server 2008 R2/Server Core 2008 R2	Windows Server 2012/ Server Core 2012	Windows Server 2016/ Server Core 2016	Windows Server 2019/ Server Core 2019
手動検索、リアルタイム検索、予約検索	あり	あり	あり	あり
コンポーネントアップデート (手動および予約アップデート)	あり	あり	あり	あり
アップデートエージェント	あり	あり	あり	あり

機能	Windows OS			
	Windows Server 2008 R2/Server Core 2008 R2	Windows Server 2012/ Server Core 2012	Windows Server 2016/ Server Core 2016	Windows Server 2019/ Server Core 2019
Web レピュテーション	あり、サーバインストール時の初期設定では無効	あり、サーバインストール時の初期設定では無効	あり、サーバインストール時の初期設定では無効	あり、サーバインストール時の初期設定では無効
ダメージクリーンナップサービス	あり	あり	あり	あり
Apex One ファイアウォール	あり、サーバインストール時の初期設定では無効	あり、サーバインストール時の初期設定では無効	あり、サーバインストール時の初期設定では無効	あり、サーバインストール時の初期設定では無効
挙動監視	あり (64 ビット)、初期設定では無効	あり (64 ビット)、初期設定では無効	あり (64 ビット)、初期設定では無効	あり (64 ビット)、初期設定では無効
エージェントセルフプロテクション • レジストリキー • プロセス • サービス • ファイル保護	あり	あり	あり	あり
デバイスコントロール (不正変更防止サービス)	あり (64 ビット)、初期設定では無効	あり (64 ビット)、初期設定では無効	あり (64 ビット)、初期設定では無効	あり (64 ビット)、初期設定では無効

機能	Windows OS			
	Windows Server 2008 R2/Server Core 2008 R2	Windows Server 2012/ Server Core 2012	Windows Server 2016/ Server Core 2016	Windows Server 2019/ Server Core 2019
情報漏えい対策オプション (デバイスコントロールの情報漏えい対策オプションを含む)	あり (64 ビット)、初期設定では無効	あり (64 ビット)、初期設定では無効	あり (64 ビット)、初期設定では無効	あり (64 ビット)、初期設定では無効
不審接続監視設定	あり	あり	あり	あり
サンプル送信	あり	あり	あり	あり
POP3 メール検索	あり	あり	あり	あり
機械学習型検索	あり	あり	あり	あり
エージェントプラグインマネージャ	あり	あり	あり	あり
スタンドアロンモード	あり (Server) なし (Server Core)	あり	あり	あり
スマートフィードバック	あり	あり	あり	あり

表 5-3. デスクトッププラットフォーム上のセキュリティエージェントの機能

機能	Windows OS		
	Windows 7	Windows 8.1	Windows 10
手動検索、リアルタイム検索、予約検索	あり	あり	あり
コンポーネントアップデート (手動および予約アップデート)	あり	あり	あり

機能	WINDOWS OS		
	WINDOWS 7	WINDOWS 8.1	WINDOWS 10
アップデートエージェント	あり	あり	あり
Web レピュテーション	あり	あり、Windows UI モードでは制限付きサポートのみ	あり
ダメージクリーンナップサービス	あり	あり	あり
Apex One ファイアウォール	あり	あり	あり
挙動監視	あり (32 ビット)	あり (32 ビット)	あり (32 ビット)
	あり (64 ビット)	あり (64 ビット)	あり (64 ビット)
エージェントセルフプロテクション • レジストリキー • プロセス • サービス • ファイル保護	あり	あり	あり
デバイスコントロール	あり (32 ビット)	あり (32 ビット)	あり (32 ビット)
(不正変更防止サービス)	あり (64 ビット)	あり (64 ビット)	あり (64 ビット)
情報漏えい対策オプション (デバイスコントロールの情報漏えい対策オプションを含む)	あり (32 ビット)	あり (32 ビット)	あり (32 ビット)
	あり (64 ビット)	あり (64 ビット)、デスクトップモードの場合	あり (64 ビット)
不審接続監視設定	あり	あり	あり
サンプル送信	あり	あり	あり
POP3 メール検索	あり	あり	あり

機能	Windows OS		
	Windows 7	Windows 8.1	Windows 10
機械学習型検索	あり	あり	あり
エージェントプラグインマネージャ	あり	あり	あり
スタンドアロンモード	あり	あり	あり
スマートフィードバック	あり	あり	あり

セキュリティエージェントのインストールと IPv6 のサポート

ここでは、デュアルスタックエンドポイントまたは IPv6 シングルスタックエンドポイントにセキュリティエージェントをインストールする際の注意事項について説明します。

インストール方法

IPv6 シングルスタックセキュリティエージェントまたはデュアルスタックエージェントにセキュリティエージェントをインストールする際には、すべてのセキュリティエージェントインストール方法を使用できます。一部のインストール方法には、セキュリティエージェントを正常にインストールするための特別な要件があります。

ServerProtect 一般サーバ移行ツールでは IPv6 アドレス指定がサポートされていないため、このツールを使用して ServerProtect をセキュリティエージェントに移行することはできません。

表 5-4. インストール方法と IPv6 のサポート

インストール方法	要件/注意事項
Web インストールページおよびブラウザベースのインストール	インストールページの URL には、Apex One サーバのホスト名または IP アドレスが含まれます。 IPv6 シングルスタックセキュリティエージェントにインストールする場合、サーバはデュアルスタックまたは IPv6 シングルスタックでなければならず、そのホスト名または IPv6 アドレスが URL に含まれている必要があります。 デュアルスタックセキュリティエージェントの場合、インストールステータス画面に表示される IPv6 アドレスは、[エージェント] > [グローバルエージェント設定] の [ネットワーク] タブの [優先 IP アドレス] セクションで選択したオプションによって異なります。
エージェントパッケージャ	エージェントパッケージャツールを実行する場合は、アップデートエージェントの権限をセキュリティエージェントに割り当てるかどうかを選択する必要があります。IPv6 シングルスタックのアップデートエージェントがアップデートを配信できるのは、IPv6 シングルスタックまたはデュアルスタックのセキュリティエージェントのみです。
セキュリティコンプライアンス、脆弱性検索ツール、リモートインストール	IPv6 シングルスタックサーバは、IPv4 シングルスタックエンドポイントにセキュリティエージェントをインストールできません。同様に、IPv4 シングルスタックサーバは、IPv6 シングルスタックエンドポイントにセキュリティエージェントをインストールできません。

エージェント IP アドレス

IPv6 アドレス指定をサポートする環境にインストールされた Apex One サーバで管理できるセキュリティエージェントは次のとおりです。

- IPv6 シングルスタックホストコンピュータにインストールされた Apex One サーバでは、IPv6 シングルスタックエージェントを管理できます。
- デュアルスタックホストコンピュータにインストールされ、IPv4 アドレスと IPv6 アドレスの両方を割り当てられている Apex One サーバでは、IPv6 シングルスタック、デュアルスタック、IPv4 シングルスタックの各エージェントを管理できます。

エージェントをインストールまたはバージョンアップすると、そのエージェントは IP アドレスを使用してサーバに登録されます。

- IPv6 シングルスタックエージェントは、IPv6 アドレスを使用して登録されます。
- IPv4 シングルスタックエージェントは、IPv4 アドレスを使用して登録されます。
- デュアルスタックエージェントは、IPv4 アドレスまたは IPv6 アドレスのいずれかを使用して登録されます。これらのエージェントが使用する IP アドレスを選択できます。

サーバへの登録時にデュアルスタックエージェントが使用する IP アドレスの設定

この設定は、デュアルスタック Apex One サーバのみで指定でき、デュアルスタックエージェントのみに適用されます。

手順

1. [エージェント] > [グローバルエージェント設定] に移動します。
2. [ネットワーク] タブをクリックします。
3. [優先 IP アドレス] セクションに移動します。
4. 次のオプションから選択します。
   - IPv4 のみ: エージェントは IPv4 アドレスを使用します。
   - 最初に IPv4、次に IPv6: エージェントは、最初に IPv4 アドレスを使用します。IPv4 アドレスを使用して登録できなかった場合は、IPv6 アドレスを使用します。どちらの IP アドレスを使用しても登録できなかった場合、エージェントは、この選択の IP アドレスの優先順位を使用して登録を再試行します。
   - 最初に IPv6、次に IPv4: エージェントは、最初に IPv6 アドレスを使用します。IPv6 アドレスを使用して登録できなかった場合は、IPv4 アドレスを使用します。どちらの IP アドレスを使用しても登録できなかった場合、エージェントは、この選択の IP アドレスの優先順位を使用して登録を再試行します。

5. [保存]をクリックします。

配信時の注意事項

このセクションでは、セキュリティエージェントの新規インストールを実行するさまざまな方法について概要を説明します。すべてのインストール方法で、対象コンピュータのローカル管理者権限が必要になります。

エージェントをインストールする場合、IPv6 のサポートを有効にするには、141 ページの「セキュリティエージェントのインストールと IPv6 のサポート」に記載されているガイドラインを参照してください。

表 5-5. インストールに関する配信時の注意事項

インストール方法/OS サポート	配信時の注意事項					
	WAN 配信	集中管理	ユーザ操作が必要	IT リソースが必要	大量配信	帯域幅の消費
Web インストールページ Windows Server Core プラットフォームではサポート対象外	なし	なし	あり	なし	なし	多い
メールリンク (インストール) Windows Server Core プラットフォームではサポート対象外	なし	なし	あり	あり	なし	多い (複数のインストールが同時に開始される場合)
UNC ベースのインストール すべての OS でサポート	なし	なし	あり	あり	なし	多い (複数のインストールが同時に開始される場合)

インストール方法/OS サポート	配信時の注意事項					
	WAN 配信	集中管理	ユーザ操作が必要	IT リソースが必要	大量配信	帯域幅の消費
リモートインストール 次を除くすべての OS でサポート: • Windows 7 Home Basic/ Home Premium • Windows 8.1 (通常版) • Windows 10 Home Edition	なし	あり	なし	あり	なし	多い
ログオンスクリプトウィザード すべての OS でサポート	なし	なし	あり	あり	なし	多い (複数のインストールが同時に開始される場合)
エージェントパッケージャ すべての OS でサポート	なし	なし	あり	あり	なし	少ない (予約されている場合)
エージェントパッケージャ (Microsoft SMS を使用して配信される MSI パッケージ) すべての OS でサポート	あり	あり	あり/なし	あり	あり	少ない (予約されている場合)

インストール方法/OS サポート	配信時の注意事項					
	WAN 配信	集中管理	ユーザ操作が必要	IT リソースが必要	大量配信	帯域幅の消費
エージェントパッケージャ (Active Directory を使用して配信される MSI パッケージ) すべての OS でサポート	あり	あり	あり/なし	あり	あり	多い (複数のインストールが同時に開始される場合)
エージェントのディスクイメージ すべての OS でサポート	なし	なし	なし	あり	なし	低
トレンドマイクロ脆弱性検索ツール (TMVS) 次を除くすべての OS でサポート: • Windows 8.1 (通常版) • Windows 10 Home Edition	なし	あり	なし	あり	なし	多い

インストール方法/OS サポート	配信時の注意事項					
	WAN 配信	集中管理	ユーザ操作が必要	IT リソースが必要	大量配信	帯域幅の消費
セキュリティコンプライアンスのインストール 次を除くすべての OS でサポート: • Windows 7 Home Basic/ Home Premium • Windows 8.1 (通常版) • Windows 10 Home Edition	なし	あり	なし	あり	なし	多い

Web インストールページからのインストール

手順

1. サポートされる Web ブラウザを開き、次の URL を入力します。

   `https://<Apex One サーバ名>:<ポート番号>/officescan`

2. ログオンページの [インストーラ] リンクをクリックして、OS に応じて 32 ビットまたは 64 ビットの MSI パッケージをダウンロードします。

3. インストールが完了すると、Windows のタスクトレイにセキュリティエージェントのアイコンが表示されます。

注意

タスクトレイに表示されるアイコンの一覧については、664 ページの「セキュリティエージェントのアイコン」を参照してください。

メールリンク (インストール)

セキュリティエージェントをインストールするようネットワーク上のユーザに指示するメールメッセージを設定します。ユーザは、このメールに記載されているセキュリティエージェントインストーラのリンクをクリックしてインストールを開始します。

セキュリティエージェントをインストールする前に、次の処理を実行します。

- セキュリティエージェントのインストール要件を確認します。
- セキュリティ上の脅威から現在保護されていないネットワーク上のコンピュータを識別します。次のタスクを実行します。
  - トレンドマイクロ脆弱性検索ツールを実行します。このツールは、指定された IP アドレス範囲に基づき、インストールされているウイルス対策ソフトウェアについてエンドポイントを分析します。

    詳細については、168 ページの「脆弱性検索ツールの使用方法」を参照してください。
  - セキュリティコンプライアンスを実行します。

    詳細については、707 ページの「管理対象外のエンドポイントに関するセキュリティコンプライアンス」を参照してください。

メールリンクの送信

IPv6 シングルスタックエージェントにインストールする場合、サーバはデュアルスタックまたは IPv6 シングルスタックでなければならず、そのホスト名または IPv6 アドレスが URL に含まれている必要があります。

デュアルスタックエージェントの場合、インストールステータス画面に表示される IPv6 アドレスは、[エージェント] > [グローバルエージェント設定] の

[ネットワーク] タブの [優先 IP アドレス] で選択したオプションによって異なります。

詳細については、142 ページの「エージェント IP アドレス」を参照してください。

手順

1. [エージェント] > [エージェントのインストール] > [メールリンク] に移動します。
2. 必要に応じてメールメッセージの件名を修正します。
3. [メールの作成] をクリックします。

   初期設定のメールプログラムが起動します。
4. 目的の受信者にメールを送信します。

UNC ベースのインストールの実行

`AutoPcc.exe` は、保護されていないエンドポイントにセキュリティエージェントをインストールし、プログラムファイルとコンポーネントをアップデートするスタンドアロンプログラムです。UNC (Uniform Naming Convention) パスを使用して AutoPcc を実行するには、エンドポイントが対象ドメインのメンバーである必要があります。

手順

1. [エージェント] > [エージェントのインストール] > [UNC ベース] に移動します。
   - `AutoPcc.exe` を使用して保護されていないエンドポイントにセキュリティエージェントをインストールするには
     a. サーバコンピュータに接続します。次の UNC パスに移動します。

        `¥¥<サーバコンピュータ名>¥ofcscan`

b. AutoPcc.exe を右クリックして、[管理者として実行] を選択します。

- リモートデスクトップを使用して AutoPcc.exe インストールを実行するには

  a. コンソールモードでリモートデスクトップ接続 (Mstsc.exe) を開きます。これにより、AutoPcc.exe のインストールがセッション 0 で実行されるようになります。

  b. ¥¥<サーバコンピュータ名>¥ofcscan ディレクトリに移動して、AutoPcc.exe を実行します。

Apex One Web コンソールからのリモートインストール

セキュリティエージェントを、ネットワークに接続された 1 台以上のエンドポイントにリモートインストールします。リモートインストールを行うためには、インストール先エンドポイントに対して管理者権限が必要です。リモートインストールでは、すでに Apex One サーバが動作しているエンドポイントには、セキュリティエージェントはインストールされません。

注意

このインストール方法は、Windows 7 Home Basic および Home Premium Edition (32 ビットバージョンと 64 ビットバージョン)、Windows 8.1 (通常版の 32 ビットバージョンと 64 ビットバージョン)、または Windows 10 Home Edition が動作しているエンドポイントでは使用できません。IPv6 シングルスタックサーバは、IPv4 シングルスタックエージェントにセキュリティエージェントをインストールできません。同様に、IPv4 シングルスタックサーバは、IPv6 シングルスタックエージェントにセキュリティエージェントをインストールできません。

手順

1. 次のインストール前タスクを実行します。

   a. ビルトインのドメイン管理者アカウントを有効にして、そのアカウントのパスワードを設定します。

b. [スタート] > [プログラム] > [管理ツール] > [セキュリティが強化された Windows ファイアウォール] に移動します。

c. ネットワーク環境に応じて、「ドメイン」、「プライベート」、「パブリック」の [ファイルとプリンタの共有] の規則を有効にします。

d. Microsoft 管理コンソールを開いて ([スタート] > [ファイル名を指定して実行] の順にクリックして「`services.msc`」と入力)、Remote Registry サービスおよび Remote Procedure Call サービスを開始します。セキュリティエージェントのインストール時には、ビルトインの管理者アカウントとパスワードを使用します。

2. Web コンソールで、[エージェント] > [エージェントのインストール] > [リモート] に移動します。

3. インストール先エンドポイントを選択します。

   - [ドメインとエンドポイント] リストに、ネットワーク上のすべての Windows ドメインが表示されます。ドメインのエンドポイントを表示するには、ドメイン名をダブルクリックします。エンドポイントを選択して、[追加] をクリックします。
   - 特定のエンドポイント名を指定するには、そのエンドポイント名をページ最上部の [エンドポイントの検索] に入力して <ENTER> キーを押します。

   対象エンドポイントのユーザ名とパスワードを入力するよう求めるメッセージが表示されます。管理者アカウントのユーザ名とパスワードを使用して、続行してください。

4. ユーザ名とパスワードを入力し、[ログオン] をクリックします。

   対象エンドポイントが、「選択済みのエンドポイント」テーブルに表示されます。

5. さらにエンドポイントを追加するには、手順 3 と 4 を繰り返します。

6. セキュリティエージェントをインストール先エンドポイントにインストールする準備ができたら、[インストール] をクリックします。

   確認画面が表示されます。

7. [はい] をクリックして、セキュリティエージェントをインストール先エンドポイントにインストールすることを確認します。

各対象エンドポイントにプログラムファイルがコピーされ、進捗状況画面が表示されます。

対象エンドポイントへのインストールが完了すると、ダイアログが表示されます。

[OK] をクリックし、ダイアログを閉じてリモートインストールは完了です。また、[選択済みのエンドポイント] リストで結果を確認することができます。

注意

複数のエンドポイントにインストールする場合、失敗したインストールがあればログに記録されますが (詳細については 788 ページの「新規インストールログ」を参照)、他のインストールは続行します。[インストール] をクリックした後は、インストールを監視する必要はありません。後でログをチェックして、インストール結果を確認してください。

トラブルシューティングについては、次の製品 Q&A の記事を参照してください。

- https://success.trendmicro.com/jp/solution/1313828

ログオンスクリプトウィザードを使用したインストール

ログオンスクリプトウィザードでは、保護されていないエンドポイントがネットワークにログオンする際にセキュリティエージェントを自動インストールします。ログオンスクリプトウィザードでは、`AutoPcc.exe` と呼ばれるプログラムをサーバログインスクリプトに追加します。

`AutoPcc.exe` は、管理対象外のエンドポイントにセキュリティエージェントをインストールし、プログラムファイルとコンポーネントをアップデートします。ログオンスクリプトを使用して AutoPcc を実行するには、エンドポイントが対象ドメインのメンバーである必要があります。

セキュリティエージェントのインストール

`AutoPcc.exe` は、自動的にはセキュリティエージェントをエンドポイントにインストールしません。ユーザはサーバコンピュータに接続し、`¥¥<サーバコ`

ンピュータ名>¥ofcscan に移動して AutoPcc.exe を右クリックし、[管理者として実行] を選択する必要があります。

AutoPcc.exe を使用したリモートデスクトップインストールの場合

- エンドポイントを Mstsc.exe /console モードで実行する必要があります。これにより、AutoPcc.exe のインストールがセッション 0 で実行されるようになります。
- 「ofcscan」フォルダにドライブをマップし、そこから AutoPcc.exe を実行します。

プログラムとコンポーネントのアップデート

AutoPcc.exe は、プログラムファイルとウイルス対策コンポーネント、スパイウェア対策コンポーネント、およびダメージクリーンナップサービスコンポーネントをアップデートします。

Windows Server スクリプト

既存のログオンスクリプトがすでにある場合は、ログオンスクリプトウィザードによって AutoPcc.exe を実行するコマンドが末尾に追加されます。ない場合は、AutoPcc.exe を実行するコマンドが含まれた ofcscan.bat という名前のバッチファイルが Apex One によって作成されます。

ログオンスクリプトウィザードによって、スクリプトの末尾に次のコマンドが追加されます。

¥¥<サーバ名>¥ofcscan¥autopcc

説明:

- <サーバ名>は、Apex One サーバコンピュータのエンドポイント名または IP アドレスです。
- 「ofcscan」は、サーバ上の Apex One 共有フォルダ名です。
- 「autopcc」は、セキュリティエージェントをインストールする autopcc 実行可能ファイルへのリンクです。

ログオンスクリプトの場所 (ネットログオン共有ディレクトリ経由):

- Windows Server 2012:¥¥Windows 2012 server¥system drive ¥windir¥sysvol¥domain¥scripts¥ofcscan.bat
- Windows Server 2016:¥¥Windows 2016 server¥system drive ¥windir¥sysvol¥domain¥scripts¥ofcscan.bat
- Windows Server 2019: ¥¥Windows 2019 server¥system drive ¥windir¥sysvol¥domain¥scripts¥ofcscan.bat

ログオンスクリプトウィザードを使用したログオンスクリプトへの Autopcc.exe の追加

手順

1. サーバインストールの実行に使用したエンドポイントで、Windows の [スタート] メニューから [プログラム] > [Trend Micro Apex One サーバ-<サーバ名>] > [システムログオンスクリプト] の順にクリックします。

   ログオンスクリプトウィザードユーティリティがロードされます。コンソールに、ネットワーク上のすべてのドメインを示すツリーが表示されます。

2. ログオンスクリプトを変更するサーバを探して選択し、[選択] をクリックします。選択したサーバがプライマリドメインコントローラであり、そのサーバに対して管理者権限を持っていることを確認します。

   ダイアログが表示され、ユーザ名とパスワードを入力するよう求められます。

3. ユーザ名とパスワードを入力します。[OK] をクリックして操作を続行します。

   [ユーザの選択] 画面が表示されます。[ユーザ] リストには、サーバにログオンするユーザのプロファイルが表示されます。[選択したユーザ] リストには、ログオンスクリプトを変更するユーザのプロファイルが表示されます。

4. 1 つのユーザプロファイルのログオンスクリプトを変更するには、[ユーザ] リストからそのユーザプロファイルを選択して、[追加] をクリックします。

5. すべてのユーザのログオンスクリプトを変更するには、[すべて追加] をクリックします。
6. 前に選択したユーザプロファイルを除外するには、[選択したユーザ] リストで名前を選択して、[削除] をクリックします。
7. 選択内容をリセットするには、[すべて削除] をクリックします。
8. 対象ユーザのプロファイルがすべて [選択したユーザ] リストにある場合は、[適用] をクリックします。

   サーバのログオンスクリプトが正常に変更されたことを示すメッセージが表示されます。
9. [OK] をクリックします。

   ログオンスクリプトウィザードがその初期画面に戻ります。
10. 他のサーバのログオンスクリプトを変更するには、ステップ 2～4 を繰り返します。
11. ログオンスクリプトウィザードを閉じるには、[終了] をクリックします。

エージェントパッケージャを使用したインストール

エージェントパッケージャでは、CD-ROM のような従来のメディアを使用してユーザに配信できるインストールパッケージが作成されます。ユーザは、エージェントエンドポイントでそのパッケージを実行して、セキュリティエージェントのインストールやバージョンアップ、およびコンポーネントのアップデートを行います。

エージェントパッケージャは、セキュリティエージェントやコンポーネントを、帯域幅が十分でない遠隔地のオフィス内のエンドポイントに配信する場合に特に便利です。エージェントパッケージャを使用してインストールされたセキュリティエージェントは、パッケージが作成されたサーバに対してレポートを送信します。

エージェントパッケージャには次のアイテムが必要です。

- 800MB のハードディスク空き容量

- Windows Installer 2.0 (MSI パッケージを実行)

トラブルシューティングについては、次の製品 Q&A の記事を参照してください。

- https://success.trendmicro.com/jp/solution/1313828

パッケージ配信のガイドライン

パッケージをユーザに送信し、使用しているエンドポイント上でセキュリティエージェントパッケージを実行するように指示します。

注意

パッケージを作成したサーバにレポートするセキュリティエージェントのユーザにのみ、パッケージを送信してください。

- EXE パッケージの場合は、インストーラファイルを右クリックして [管理者として実行] をクリックします。
- MSI パッケージの場合:
  1. 次のタスクを実行してパッケージを配信します。
     - 161 ページの「Active Directory を使用した MSI パッケージの配信」
     - 162 ページの「Microsoft SMS を使用した MSI パッケージの配信」
  2. コマンドプロンプトウィンドウから MSI パッケージを起動して、リモートエンドポイントへのセキュリティエージェントのサイレントインストールを実行します。

エージェントパッケージの検索方法に関するガイドライン

パッケージの検索方法を選択します。詳細については、279 ページの「検索方法の種類」を参照してください。

選択した検索方法によって、パッケージに含まれるコンポーネントは異なります。それぞれの検索方法で使用可能なコンポーネントの詳細については、

231 ページの「セキュリティエージェントのアップデート」を参照してください。

検索方法を選択する前に、パッケージの効率的な配信に役立つ次のガイドラインに注目してください。

- パッケージを使用して、エージェントをこの Apex One のバージョンにバージョンアップする場合は、Web コンソールでドメインレベルの検索方法を確認してください。コンソールで [エージェント] > [エージェント管理] に移動して、エージェントが属するエージェントツリードメインを選択し、[設定] > [検索設定] > [検索方法] の順にクリックします。ドメインレベルの検索方法とパッケージの検索方法は、一致している必要があります。

- パッケージを使用して、セキュリティエージェントの新規インストールを実行する場合は、エージェントのグループ設定を確認してください。Web コンソールで、[エージェント] > [エージェントのグループ設定] に移動します。

- エージェントのグループ設定が NetBIOS、Active Directory、または DNS ドメインに基づいている場合は、対象エンドポイントが属しているドメインを確認します。存在する場合は、そのドメインに設定されている検索方法を確認します。ドメインが存在しない場合は、エージェントツリーでルートドメインアイコン () を選択して [設定] > [検索設定] > [検索方法] の順にクリックし、ルートレベルの検索方法を確認します。ドメインまたはルートレベルの検索方法とパッケージの検索方法は、一致している必要があります。

- エージェントのグループ設定がカスタムエージェントグループに基づいている場合は、[グループ設定の優先順位] と [アップデート元] を確認します。

  対象エンドポイントが特定のアップデート元に属している場合は、対応する [宛先] を確認します。宛先は、エージェントツリーに表示されるドメイン名です。エージェントは、インストール後にそのドメインの検索方法を適用します。

- パッケージを使用して、エージェントのコンポーネントをこの Apex One のバージョンでアップデートする場合は、エージェントが属するエージェントツリードメインに設定されている検索方法を確認してくださ

い。ドメインレベルの検索方法とパッケージの検索方法は、一致している必要があります。

エージェントパッケージャを使用したインストールパッケージの作成

手順

1. Apex One サーバコンピュータで、<サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility¥ClientPackager に移動します。
2. ClnPack.exe をダブルクリックして、ツールを実行します。

   エージェントパッケージャコンソールが開きます。
3. 作成するパッケージの種類を選択します。

   表 5-6. エージェントパッケージの種類

パッケージの種類	説明
セットアップ	パッケージを実行可能ファイルとして作成する場合に選択します。このパッケージは、現在サーバで使用可能なコンポーネントを含むセキュリティエージェントプログラムをインストールします。対象エンドポイントに前のバージョンのエージェントがインストールされている場合、この実行可能ファイルを実行するとエージェントがバージョンアップされます。
アップデート	現在サーバで使用可能なコンポーネントを含むパッケージを作成する場合に選択します。パッケージは実行可能ファイルとして作成されます。エージェントエンドポイントでコンポーネントをアップデートする際に問題が発生する場合には、このパッケージを使用します。
MSI	Microsoft Installer Package 形式に準拠するパッケージを作成する場合に選択します。このパッケージも、現在サーバで使用可能なコンポーネントを含むセキュリティエージェントプログラムをインストールします。対象エンドポイントに前のバージョンのエージェントがインストールされている場合、この MSI ファイルを実行するとエージェントがバージョンアップされます。

4. パッケージを作成する対象となる OS を選択します。作成したパッケージは、ここで選択した OS を実行するエンドポイントにのみ配信してください。別の種類の OS を対象に配信するには、別のパッケージを作成します。

5. エージェントパッケージで配信する検索方法を選択します。

   検索方法を選択する際のガイドラインは、156 ページの「エージェントパッケージの検索方法に関するガイドライン」を参照してください。

6. [ドメイン] で、次のいずれかを選択します。

   - エージェントによるドメインの自動報告を許可する: セキュリティエージェントのインストール後、エージェントは Apex One サーバデータベースにクエリを送信し、そのドメイン設定をサーバに報告します。
   - リスト内の任意のドメイン: エージェントパッケージャが Apex One サーバと同期し、エージェントツリーで現在使用されているドメインを表示します。

7. [オプション] で、次の項目から選択します。

オプション	説明
サイレントモード	このオプションを選択すると、エージェントエンドポイントにバックグラウンドでインストールするパッケージが作成されます。エージェントにインストールが通知されることはなく、インストールステータスウィンドウも表示されません。パッケージをリモートで対象エンドポイントに配布する場合は、このオプションを有効にします。
最新バージョンで上書きする	このオプションを選択すると、エージェントのコンポーネントバージョンが、現在サーバで使用可能なバージョンで上書きされます。このオプションを有効にすると、サーバとエージェントのコンポーネントが同期されます。
事前検索を無効にする (新規インストールのみ)	対象エンドポイントにセキュリティエージェントがインストールされていない場合、セキュリティエージェントのインストールを実行する前にエンドポイントのセキュリティリスクが検索されます。対象エンドポイントがセキュリティリスクに感染していないことが明らかな場合は、事前検索を無効にします。

オプション	説明
	事前検索を有効にすると、次に示すエンドポイント上の最も攻撃を受けやすい領域でウイルス/不正プログラムが検索されます。 • システム領域とシステムディレクトリ (システム領域感染型ウイルスが対象) • Windows フォルダ • Program Files フォルダ

8. [アップデートエージェントの機能] で、アップデートエージェントが配信できる機能を選択します。

9. [コンポーネント] で、パッケージに含めるコンポーネントおよび機能を選択します。

   - コンポーネントの詳細については、204 ページの「Apex One のコンポーネントとプログラム」を参照してください。
   - 情報漏えい対策オプションモジュールは、情報漏えい対策オプションをインストールしてアクティベートした場合にのみ選択できます。情報漏えい対策オプションの詳細については、83 ページの情報漏えい対策オプションの使用開始を参照してください。

10. [入力ファイル] で、`ofcscan.ini` ファイルの場所が正しいことを確認します。パスを変更するには、[...] をクリックして `ofcscan.ini` ファイルを参照します。

    初期設定では、このファイルは Apex One サーバの<サーバインストールフォルダ>¥PCCSRV フォルダにあります。

11. [出力ファイル] で ([...]) をクリックして、セキュリティエージェントパッケージを作成する場所を指定し、パッケージファイル名 (例: `AgentSetup.exe`) を入力します。

12. [作成] をクリックします。

    パッケージが作成されると、「パッケージが作成されました。」というメッセージが表示されます。前の手順で指定したディレクトリでパッケージを探します。

13. パッケージを配信します。

Active Directory を使用した MSI パッケージの配信

Active Directory の機能を利用すれば、複数のセキュリティエージェントエンドポイントに MSI パッケージを同時に配信することができます。

MSI ファイルの作成手順については、155 ページの「エージェントパッケージャを使用したインストール」を参照してください。

手順

1. 次の手順を実行します。
   - Windows Server 2008 R2 の場合:
     a. グループポリシー管理コンソールを開きます。[スタート] > [コントロール パネル] > [管理ツール] > [グループ ポリシーの管理] の順にクリックします。
     b. コンソールツリーで、編集する GPO が含まれているフォレストおよびドメイン内の [グループ ポリシー オブジェクト] を展開します。
     c. 編集する GPO を右クリックして、[編集] をクリックします。これにより、グループポリシーオブジェクトエディタが開きます。
   - Windows Server 2012 以降の場合:
     a. グループポリシー管理コンソールを開きます。[サーバ管理] > [ツール] > [グループ ポリシーの管理] の順にクリックします。
     b. コンソールツリーで、編集する GPO が含まれているフォレストおよびドメイン内の [グループ ポリシー オブジェクト] を展開します。
     c. 編集する GPO を右クリックして、[編集] をクリックします。これにより、グループポリシーオブジェクトエディタが開きます。
2. [コンピュータの構成] または [ユーザの構成] のいずれかを選択して、その下にある [ソフトウェアの設定] を開きます。

ヒント

エンドポイントにログオンするユーザの種類に関係なく MSI パッケージをインストールするために、[ユーザの構成] ではなく [コンピュータの構成] を使用することをお勧めします。

3. [ソフトウェアの設定] で、[ソフトウェア インストール] を右クリックして、[新規作成] および [パッケージ] を選択します。
4. MSI パッケージを探して選択します。
5. 配信方法を選択して、[OK] をクリックします。
   - 割り当て: MSI パッケージは、ユーザが次回エンドポイントにログオンするとき ([ユーザの構成] を選択した場合)、またはエンドポイントが再起動するとき ([コンピュータの構成] を選択した場合) に、自動的に配信されます。この方法では、ユーザの操作は必要ありません。
   - 公開: MSI パッケージを実行するには、[コントロール パネル] に進み、[プログラムの追加と削除] 画面を開き、ネットワーク上のプログラムを追加/インストールするオプションを選択するようにユーザに通知します。セキュリティエージェントの MSI パッケージが表示されたら、ユーザはセキュリティエージェントのインストールを続行できます。

Microsoft SMS を使用した MSI パッケージの配信

サーバに Microsoft BackOffice SMS がインストールされている場合は、Microsoft SMS (Systems Management Server) を使用して、MSI パッケージを配信します。

MSI ファイルの作成手順については、155 ページの「エージェントパッケージャを使用したインストール」を参照してください。

SMS サーバでは、パッケージを対象エンドポイントに配信する前に、Apex One サーバから MSI ファイルを取得する必要があります。

- ローカル:SMS サーバと Apex One サーバが、同一エンドポイント上にある場合です。

- リモート:SMS サーバと Apex One サーバが、異なるエンドポイント上にある場合です。

Microsoft SMS を使用してインストールする場合の既知の問題:

- SMS コンソールの [実行時間] 列に「不明」と表示されます。
- インストールが成功しなかった場合でも、インストールステータスは、SMS プログラムモニタ上でインストールが完了したことを示す場合があります。

  インストールが正常に完了したかどうかを確認する方法については、196 ページの「インストール後の確認」を参照してください。

以下の手順は、Microsoft SMS 2.0 および 2003 を使用する場合を対象としています。

パッケージのローカルでの取得

手順

1. SMS 管理コンソールを開きます。
2. [ツリー] タブの [パッケージ] をクリックします。
3. [操作] メニューから、[新規作成] > [定義に基づくパッケージ] の順にクリックします。

   定義に基づくパッケージの作成ウィザードの [ようこそ] 画面が表示されます。
4. [次へ] をクリックします。

   [パッケージ定義] 画面が表示されます。
5. [参照] をクリックします。

   [ファイルを開く] 画面が表示されます。
6. エージェントパッケージャによって作成された EXE パッケージファイルを参照して選択し、[ファイルを開く] をクリックします。

[パッケージ定義] 画面に、EXE パッケージ名が表示されます。パッケージには、「セキュリティエージェント」とプログラムのバージョンが表示されています。

7. [次へ] をクリックします。

   [ソース ファイル] 画面が表示されます。

8. [常にソース ディレクトリからファイルを取得する] をクリックし、[次へ] をクリックします。

   [ソース ディレクトリ] 画面が表示されます。この画面には、作成するパッケージの名前とソースディレクトリが表示されています。

9. [サイト サーバのローカル ドライブ] をクリックします。

10. [参照] をクリックして、EXE ファイルが含まれているソースディレクトリを選択します。

11. [次へ] をクリックします。

    ウィザードによりパッケージが作成されます。パッケージの作成が完了すると、パッケージの名前が SMS 管理コンソールに表示されます。

パッケージのリモートでの取得

手順

1. Apex One サーバで、エージェントパッケージャを使用し、EXE 拡張子が付いたセットアップパッケージを作成します (MSI パッケージは作成できません)。詳細については、155 ページの「エージェントパッケージャを使用したインストール」を参照してください。

2. パッケージャを格納するためにエンドポイントで、共有フォルダを作成します。

3. SMS 管理コンソールを開きます。

4. [ツリー] タブの [パッケージ] をクリックします。

5. [操作] メニューから、[新規作成] > [定義に基づくパッケージ] の順にクリックします。

定義に基づくパッケージの作成ウィザードの [ようこそ] 画面が表示されます。

6. [次へ] をクリックします。

   [パッケージ定義] 画面が表示されます。

7. [参照] をクリックします。

   [ファイルを開く] 画面が表示されます。

8. MSI パッケージファイルを参照します。MSI パッケージファイルは、作成した共有フォルダにあります。

9. [次へ] をクリックします。

   [ソース ファイル] 画面が表示されます。

10. [常にソース ディレクトリからファイルを取得する] をクリックし、[次へ] をクリックします。

    [ソース ディレクトリ] 画面が表示されます。

11. [ネットワーク パス (UNC 名)] をクリックします。

12. [参照] をクリックして、MSI ファイルが含まれているソースディレクトリ (作成した共有フォルダ) を選択します。

13. [次へ] をクリックします。

    ウィザードによりパッケージが作成されます。パッケージの作成が完了すると、パッケージの名前が SMS 管理コンソールに表示されます。

対象エンドポイントへのパッケージの配信

手順

1. [ツリー] タブの [提供情報] をクリックします。

2. [操作] メニューから、[すべてのタスク] > [ソフトウェアの配布] の順にクリックします。

   ソフトウェアの配布ウィザードの [ようこそ] 画面が表示されます。

3. [次へ] をクリックします。

   [パッケージ] 画面が表示されます。

4. [既存のパッケージを配布する] をクリックし、作成したセットアップパッケージの名前をクリックします。

5. [次へ] をクリックします。

   [配布ポイント] 画面が表示されます。

6. パッケージをコピーする配布ポイントを選択し、[次へ] をクリックします。

   [プログラムの提供] 画面が表示されます。

7. セキュリティエージェントのセットアップパッケージを提供するには、[はい] をクリックしてから [次へ] をクリックします。

   [提供情報のターゲット] 画面が表示されます。

8. [参照] をクリックして対象エンドポイントを選択します。

   [コレクションの参照] 画面が表示されます。

9. [すべての Windows NT システム] をクリックします。

10. [OK] をクリックします。

    [提供情報のターゲット] 画面が再度表示されます。

11. [次へ] をクリックします。

    [提供情報の名前] 画面が表示されます。

12. テキストボックスに提供情報の名前とコメントを入力して、[次へ] をクリックします。

    [サブコレクションへの提供] 画面が表示されます。

13. パッケージをサブコレクションに提供するかどうかを決定します。指定したコレクションのメンバーだけにプログラムを提供するか、またはサブコレクションのメンバーにプログラムを提供するかを選択できます。

14. [次へ] をクリックします。

[提供情報のスケジュール] 画面が表示されます。

15. 日時を入力するか選択して、セキュリティエージェントセットアップパッケージをいつ提供するかを指定します。

注意

特定の日付にパッケージの提供を停止するように Microsoft SMS を設定するには、[はい] をクリックします。この提供情報に有効期限を設定する場合、[有効期限の日時] のリストボックスで日時を指定します。

---

16. [次へ] をクリックします。

    [プログラムの割り当て] 画面が表示されます。

17. [はい、プログラムを割り当てます] をクリックしてから [次へ] をクリックします。

    Microsoft SMS によって提供情報が作成され、SMS 管理コンソールに表示されます。

18. Microsoft SMS によって、提供されたプログラム (セキュリティエージェントプログラム) が対象エンドポイントに配布されると、対象エンドポイントごとに画面が表示されます。[はい] をクリックし、ウィザードの指示に従ってセキュリティエージェントをエンドポイントにインストールするように、ユーザに指示します。

エージェントのディスクイメージを使用したインストール

ディスクイメージング技術により、ディスクイメージングソフトウェアを使用してセキュリティエージェントのイメージを作成し、そのイメージのクローンをネットワーク上の他のコンピュータに作成できます。

サーバがエージェントを個々に識別できるように、各セキュリティエージェントのインストールでは GUID (Globally Unique Identifier) が必要になります。Apex One のプログラム `ImgSetup.exe` を使用して、クローンごとに異なる GUID を作成します。

セキュリティエージェントのディスクイメージの作成

手順

1. セキュリティエージェントをエンドポイントにインストールします。
2. `ImgSetup.exe` を、<サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility¥ImgSetup からこのエンドポイントにコピーします。
3. `ImgSetup.exe` をこのエンドポイント上で実行します。

   これにより、RUN レジストリキーが HKEY_LOCAL_MACHINE の下に作成されます。
4. ディスクイメージングソフトウェアを使用して、セキュリティエージェントのディスクイメージを作成します。
5. クローンを再起動します。

   `ImgSetup.exe` が自動的に起動され、新しい GUID 値が 1 つ作成されます。セキュリティエージェントはこの新しい GUID をサーバにレポートし、サーバは新しいセキュリティエージェントの新しいレコードを作成します。

警告!

Apex One データベースに同じ名前を持つ 2 つのコンピュータが存在しないように、複製したセキュリティエージェントのエンドポイント名またはドメイン名を手動で変更してください。

脆弱性検索ツールの使用方法

脆弱性検索ツールを使用して、インストールされているウイルス対策ソリューションを検出し、ネットワーク上の保護されていないコンピュータを検索して、コンピュータにセキュリティエージェントをインストールします。

脆弱性検索ツール使用時の注意事項

脆弱性検索ツールを使用するかどうかを決定する際には、次のことを考慮に入れてください。

ネットワーク管理

表 5-7. ネットワーク管理

環境	脆弱性検索ツールの効果
厳しいセキュリティポリシーによる管理	非常に効果的。脆弱性検索ツールはすべてのコンピュータにウイルス対策製品がインストールされているかどうかを報告します。
各拠点で管理	やや効果的
一元管理	やや効果的
アウトソーシング	やや効果的
各ユーザによるコンピュータ管理	効果なし。脆弱性検索ツールはネットワーク上のウイルス対策製品を検索するため、ユーザが各自のコンピュータを検索するのは適切ではありません。

ネットワークトポロジとアーキテクチャ

表 5-8. ネットワークトポロジとアーキテクチャ

環境	脆弱性検索ツールの効果
単一の場所	非常に効果的。脆弱性検索ツールでは、IP セグメント全体を検索して、拠点内にセキュリティエージェントを簡単にインストールできます。
高速接続の複数の場所	やや効果的
低速接続の複数の場所	効果なし。すべての場所で脆弱性検索ツールを実行する必要があり、セキュリティエージェントのインストールはローカルの Apex One サーバによって行われなければなりません。

環境	脆弱性検索ツールの効果
リモートおよび単独のコンピュータ	やや効果的

ソフトウェア/ハードウェア仕様

表 5-9. ソフトウェア/ハードウェア仕様

環境	脆弱性検索ツールの効果
Windows NT ベースの OS	非常に効果的。脆弱性検索ツールは、NT ベースの OS が動作しているコンピュータに、セキュリティエージェントを簡単にリモートインストールできます。
混合 OS	やや効果的。脆弱性検索ツールでは、Windows NT ベースの OS が動作しているコンピュータにのみインストールを実行できます。
デスクトップ管理ソフトウェア	効果なし。脆弱性検索ツールは、デスクトップ管理ソフトウェアでは使用できません。しかし、セキュリティエージェントのインストールの進捗状況追跡には役に立ちます。

ドメイン構造

表 5-10. ドメイン構造

環境	脆弱性検索ツールの効果
Microsoft Active Directory	非常に効果的。脆弱性検索ツールでドメイン管理者アカウントを指定し、セキュリティエージェントのリモートインストールを実行できるようにします。
ワークグループ	効果なし。脆弱性検索ツールでは、異なる管理アカウントとパスワードを使用したコンピュータへのインストールが困難な場合があります。
Novell™ Directory Service	効果なし。脆弱性検索ツールでは、セキュリティエージェントをインストールするために Windows ドメインアカウントが必要です。

環境	脆弱性検索ツールの効果
ピアツーピア	効果なし。脆弱性検索ツールでは、異なる管理アカウントとパスワードを使用したコンピュータへのインストールが困難な場合があります。

ネットワークトラフィック

表 5-11. ネットワークトラフィック

環境	脆弱性検索ツールの効果
LAN 接続	非常に効果的
512 Kbps	やや効果的
T1 接続以上	やや効果的
ダイヤルアップ	効果なし。セキュリティエージェントのインストールに長時間要します。

ネットワークサイズ

表 5-12. ネットワークサイズ

環境	脆弱性検索ツールの効果
大規模企業	非常に効果的。ネットワークが大きくなればなるほど、セキュリティエージェントインストールのチェックのために、脆弱性検索ツールの必要性が高まります。
中小企業	やや効果的。小規模ネットワークでは、脆弱性検索ツールによるセキュリティエージェントのインストールはオプションにできます。他のセキュリティエージェントインストール方法の方が、実装が簡単なことがあります。

脆弱性検索ツールを使用してセキュリティエージェントをインストールする際のガイドライン

次の場合、セキュリティエージェントはインストールされません。

- Apex One サーバまたは別のセキュリティソフトウェアが対象のホストコンピュータにインストールされている場合。
- リモートエンドポイントで、Windows 7 SP1 Home Basic、Windows 7 SP1 Home Premium、Windows 8.1 (通常版)、Windows 10 Home、または Windows 11 Home が実行されている場合。

注意

に記載されている別のインストール方法を使用すると、対象のホストコンピュータにセキュリティエージェントをインストールできます。

脆弱性検索ツールを使用してセキュリティエージェントをインストールする前に、次の手順を実行します。

- Windows 7 SP1 (Professional、Enterprise、Ultimate Edition)、Windows 8.1 (Pro、Enterprise)、Windows 10 (Pro、Education、Enterprise)、Windows 11 (Pro、Education、Enterprise)、またはサポート対象の Windows Server (すべてのエディション) の場合

  1. ビルトインの管理者アカウントを有効にして、そのアカウントのパスワードを設定します。
  2. [スタート] > [プログラム] > [管理ツール] > [セキュリティが強化された Windows ファイアウォール] の順にクリックします。
  3. 「ドメイン プロファイル」、「プライベート プロファイル」、および「パブリック プロファイル」で、ファイアウォールの状態をオフにします。
  4. Microsoft 管理コンソールを開いて ([スタート] > [ファイル名を指定して実行] の順にクリックして「`services.msc`」と入力)、リモートレジストリサービスを開始します。セキュリティエージェントのインストール時には、ビルトインの管理者アカウントとパスワードを使用します。

脆弱性検索の方法

脆弱性検索では、ホストコンピュータにセキュリティソフトウェアがインストールされているかどうかがチェックされ、保護されていないホストコンピュータにセキュリティエージェントをインストールすることができます。

方法	詳細
手動脆弱性検索	管理者は、手動で脆弱性検索を実行できます。
予約脆弱性検索	管理者によって設定されたスケジュールに従って、脆弱性検索が自動的に実行されます。

脆弱性検索ツールの実行が完了すると、対象のホストコンピュータ上のセキュリティエージェントのステータスが表示されます。ステータスは次のいずれかです。

- 標準:セキュリティエージェントが起動され、正常に動作しています。
- 異常:セキュリティエージェントサービスが実行されていないか、セキュリティエージェントでリアルタイム保護が実行されていません。
- インストールされていません: TMListen サービスが見つからないか、セキュリティエージェントがインストールされていません。
- 到達不能:脆弱性検索ツールは、ホストコンピュータとの接続を確立できないため、セキュリティエージェントのステータスを特定できません。

手動脆弱性検索の実行

手順

1. Apex One サーバコンピュータで脆弱性検索を実行するには、<サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility¥TMVS に移動し、TMVS.exe をダブルクリックします。トレンドマイクロ脆弱性検索ツールのコンソールが表示されます。別のエンドポイントで脆弱性検索を実行するには、以下の手順に従います。

   a. Apex One サーバコンピュータで、<サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility に移動します。

   b. TMVS フォルダを別のエンドポイントにコピーします。

   c. 別のエンドポイントで、TMVS フォルダを開いて、TMVS.exe をダブルクリックします。

      トレンドマイクロ脆弱性検索ツールのコンソールが表示されます。

注意

Terminal Server から脆弱性検索ツールを起動することはできません。

2. [手動検索] セクションに移動します。
3. チェックするエンドポイントの IP アドレス範囲を入力します。
   a. IPv4 アドレス範囲を入力します。

      注意

      IPv4 シングルスタックホストコンピュータまたはデュアルスタックホストコンピュータで脆弱性検索ツールを実行する場合、IPv4 アドレス範囲のみをクエリできます。脆弱性検索ツールでは、クラス B の IP アドレス範囲 (例: `168.212.1.1`～`168.212.254.254`) のみがサポートされます。

   b. IPv6 アドレス範囲については、IPv6 のプレフィックスおよび長さを入力します。

      注意

      IPv6 シングルスタックホストコンピュータまたはデュアルスタックホストコンピュータで脆弱性検索ツールを実行する場合、IPv6 アドレス範囲のみをクエリできます。

4. [設定] をクリックします。

   [設定] 画面が表示されます。
5. 次の設定を行います。

オプション	説明
ping 設定	脆弱性検索では、前の手順で指定した IP アドレスに対して「ping」を実施し、それらが現在使用中であるかどうかをチェックできます。対象のホストコンピュータで IP アドレスが使用されている場合、脆弱性検索ツールはホストコンピュータの OS を特定することができます。 詳細については、186 ページの「Ping 設定」を参照してください。

オプション	説明
コンピュータの説明を取得する方法	「ping」コマンドに応答するホストコンピュータの場合、脆弱性検索ツールではホストコンピュータに関する追加情報を取得できます。 詳細については、183 ページの「エンドポイントの説明を取得する方法」を参照してください。
製品名クエリ	脆弱性検索ツールでは、対象のホストコンピュータにセキュリティソフトウェアがインストールされているかどうかをチェックできます。 詳細については、179 ページの「製品クエリ」を参照してください。
Apex One サーバ設定	脆弱性検索ツールによって、保護されていないホストコンピュータにセキュリティエージェントが自動的にインストールされるようにするには、これらの設定を指定します。これらの設定は、セキュリティエージェントがホストコンピュータへのログオンに使用する管理アカウント情報を特定します。 詳細については、187 ページの「Apex One サーバの設定」を参照してください。 注意 条件によっては、対象のホストコンピュータにセキュリティエージェントがインストールされない場合があります。 詳細については、171 ページの「脆弱性検索ツールを使用してセキュリティエージェントをインストールする際のガイドライン」を参照してください。
通知	脆弱性検索ツールでは、脆弱性検索結果を Apex One 管理者に送信できます。保護されていないホストコンピュータに通知を表示することもできます。 詳細については、184 ページの「通知」を参照してください。
結果の保存	脆弱性検索では、脆弱性検索結果を管理者に送信するほか、結果を .csv ファイルに保存することもできます。 詳細については、185 ページの「脆弱性検索結果」を参照してください。

6. [OK] をクリックします。
7. [開始] をクリックします。

脆弱性検索結果が、[手動検索] タブの [結果] 表に表示されます。

8. 検索結果をカンマ区切り形式 (.csv) のファイルに保存するには、[エクスポート] をクリックして、ファイルを保存するフォルダの場所を指定し、ファイル名を入力して [保存] をクリックします。

予約脆弱性検索の設定

手順

1. Apex One サーバコンピュータで脆弱性検索を実行するには、<サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility¥TMVS に移動し、TMVS.exe をダブルクリックします。トレンドマイクロ脆弱性検索ツールのコンソールが表示されます。別のエンドポイントで脆弱性検索を実行するには、以下の手順に従います。

   a. Apex One サーバコンピュータで、<サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility に移動します。

   b. TMVS フォルダを別のエンドポイントにコピーします。

   c. 別のエンドポイントで、TMVS フォルダを開いて、TMVS.exe をダブルクリックします。

      トレンドマイクロ脆弱性検索ツールのコンソールが表示されます。

   注意

   Terminal Server から脆弱性検索ツールを起動することはできません。

2. [予約検索] セクションに移動します。
3. [追加/編集] をクリックします。

   [予約検索] 画面が表示されます。
4. 予約脆弱性検索の名前を入力します。
5. チェックするエンドポイントの IP アドレス範囲を入力します。

   a. IPv4 アドレス範囲を入力します。

注意

IPv4 シングルスタックホストコンピュータまたはデュアルスタックホストコンピュータで脆弱性検索ツールを実行する場合、IPv4 アドレス範囲のみをクエリできます。脆弱性検索ツールでは、クラス B の IP アドレス範囲 (例: 168.212.1.1～168.212.254.254) のみがサポートされます。

b. IPv6 アドレス範囲については、IPv6 のプレフィックスおよび長さを入力します。

注意

IPv6 シングルスタックホストコンピュータまたはデュアルスタックホストコンピュータで脆弱性検索ツールを実行する場合、IPv6 アドレス範囲のみをクエリできます。

6. 24 時間形式を使用して予約検索の開始時刻を指定した後、検索の実行頻度を選択します。日次、週次、月次から選択します。

7. 使用する脆弱性検索設定のセットを選択します。

   a. 手動脆弱性検索の設定を行っている場合、その設定を使用するには、[現在の設定を使用] を選択します。

   手動脆弱性検索の設定の詳細については、173 ページの「手動脆弱性検索の実行」を参照してください。

   b. 手動脆弱性検索の設定を指定していない場合、または別の設定を使用する場合は、[設定を変更] を選択して、[設定] をクリックします。

   [設定] 画面が表示されます。

   c. 次の設定を行います。

ping 設定	脆弱性検索では、前の手順で指定した IP アドレスに対して「ping」を実施し、それらが現在使用中であるかどうかをチェックできます。対象のホストコンピュータで IP アドレスが使用されている場合、脆弱性検索ツールはホストコンピュータの OS を特定することができます。 詳細については、186 ページの「Ping 設定」を参照してください。

コンピュータの説明を取得する方法	「ping」コマンドに応答するホストコンピュータの場合、脆弱性検索ツールではホストコンピュータに関する追加情報を取得できます。 詳細については、183 ページの「エンドポイントの説明を取得する方法」を参照してください。
製品名クエリ	脆弱性検索ツールでは、対象のホストコンピュータにセキュリティソフトウェアがインストールされているかどうかをチェックできます。 詳細については、179 ページの「製品クエリ」を参照してください。
Apex One サーバ設定	脆弱性検索ツールによって、保護されていないホストコンピュータにセキュリティエージェントが自動的にインストールされるようにするには、これらの設定を指定します。これらの設定は、セキュリティエージェントがホストコンピュータへのログオンに使用する管理アカウント情報を特定します。 詳細については、187 ページの「Apex One サーバの設定」を参照してください。 注意 条件によっては、対象のホストコンピュータにセキュリティエージェントがインストールされない場合があります。 詳細については、171 ページの「脆弱性検索ツールを使用してセキュリティエージェントをインストールする際のガイドライン」を参照してください。
通知	脆弱性検索ツールでは、脆弱性検索結果を Apex One 管理者に送信できます。保護されていないホストコンピュータに通知を表示することもできます。 詳細については、184 ページの「通知」を参照してください。
結果の保存	脆弱性検索では、脆弱性検索結果を管理者に送信するほか、結果を.csv ファイルに保存することもできます。 詳細については、185 ページの「脆弱性検索結果」を参照してください。

8. [OK] をクリックします。

   [予約検索] 画面が閉じます。作成した予約脆弱性検索が [予約検索] セクションに表示されます。通知を有効にした場合、脆弱性検索ツールから予約脆弱性検索の結果が送信されます。

9. 予約脆弱性検索をただちに実行するには、[すぐに実行] をクリックします。

   脆弱性検索結果が、[予約検索] タブの [結果] 表に表示されます。

10. 検索結果をカンマ区切り形式 (.csv) のファイルに保存するには、[エクスポート] をクリックして、ファイルを保存するフォルダの場所を指定し、ファイル名を入力して [保存] をクリックします。

脆弱性検索の設定

脆弱性検索の設定は、トレンドマイクロ脆弱性検索ツール (TMVS.exe) または TMVS.ini ファイルで指定します。

注意

脆弱性検索ツールのデバッグログを収集する方法については、777 ページの「LogServer.exe を使用するサーバデバッグログ」を参照してください。

製品クエリ

脆弱性検索ツールでは、エージェントにセキュリティソフトウェアがインストールされているかどうかをチェックできます。次の表では、脆弱性検索ツールによるセキュリティ製品のチェック方法を示しています。

表 5-13. 脆弱性検索ツールでチェックされるセキュリティ製品

製品	説明
ServerProtect for Windows	脆弱性検索ツールは、RPC エンドポイントを使用して、SPNTSVC.exe が動作しているかどうかをチェックします。また、OS、ウイルス検索エンジン、ウイルスパターンファイル、製品バージョンなどの情報を返します。ServerProtect インフォメーションサーバまたは ServerProtect 管理コンソールは検出できません。
ServerProtect for Linux	対象エンドポイントが Windows を実行していない場合、脆弱性検索ツールはポート 14942 に接続して、そのエンドポイントに ServerProtect for Linux がインストールされているかどうかを調べます。
セキュリティエージェント	脆弱性検索ツールは、セキュリティエージェントポートを使用して、セキュリティエージェントがインストールされているかどうかをチェックします。また、TMListen.exe プロセスが動作しているかどうかもチェックします。初期設定の場所から実行された場合は、自動的にポート番号を取得します。 Apex One サーバ以外のエンドポイントで脆弱性検索ツールを起動した場合は、他のエンドポイントの通信ポートをチェックしてから使用してください。
PortalProtect™	脆弱性検索ツールは、http://localhost:port/PortalProtect/index.html という Web ページをロードして、製品がインストールされているかどうかをチェックします。
InterScan for Microsoft Exchange	脆弱性検索ツールは、http://ipaddress:port/scanmail.html という Web ページをロードして、InterScan がインストールされているかどうかをチェックします。 InterScan で使用される初期設定のポート番号は 16372 です。InterScan で別のポート番号が使用される場合は、そのポート番号を指定してください。そうしなければ、脆弱性検索ツールが'InterScan を検出できません。

製品	説明
InterScan ファミリ	脆弱性検索ツールは、さまざまな製品の各 Web ページをロードして、製品がインストールされているかどうかをチェックします。 • InterScan Messaging Security Suite 5.x:`http://localhost:port/eManager/cgi-bin/eManager.htm` • InterScan eManager 3.x:`http://localhost:port/eManager/cgi-bin/eManager.htm` • InterScan VirusWall 3.x:`http://localhost:port/InterScan/cgi-bin/interscan.dll`
Trend Micro Internet Security (ウイルスバスター)	脆弱性検索ツールは、ポート 40116 を使用して、ウイルスバスターがインストールされているかどうかをチェックします。
McAfee VirusScan ePolicy Orchestrator	脆弱性検索ツールは、特殊なトークンを TCP ポート 8081 (サーバとエージェントを接続するための ePolicy Orchestrator の初期設定ポート) に送信します。このウイルス対策製品がインストールされているエンドポイントは、特殊なトークンタイプを使用して返信します。脆弱性検索ツールは、スタンドアロンの McAfee VirusScan を検出できません。
Norton Antivirus Corporate Edition	脆弱性検索ツールは、特殊なトークンを UPD ポート 2967 (Norton Antivirus Corporate Edition RTVScan の初期設定ポート) に送信します。このウイルス対策製品がインストールされているエンドポイントは、特殊なトークンタイプを使用して返信します。Norton Antivirus Corporate Edition は UDP を使用して通信するため、精度は保証されません。さらに、ネットワークトラフィックが UDP の待機時間に影響する場合があります。

脆弱性検索ツールでは、次のプロトコルを使用する製品とコンピュータを検出します。

- RPC:ServerProtect for Windows NT を検出します。
- UDP:Norton AntiVirus Corporate Edition クライアントを検出します。
- TCP:McAfee VirusScan ePolicy Orchestrator を検出します。
- ICMP:ICMP パケットを送信することによりコンピュータを検出します。

- HTTP:セキュリティエージェントを検出します。
- DHCP:DHCP 要求を検出すると、脆弱性検出ツールは、要求元のエンドポイントにウイルス対策ソフトウェアがインストールされているかどうかをチェックします。

製品クエリの設定

製品クエリの設定は、脆弱性検索設定のサブセットです。脆弱性検索の設定の詳細については、172 ページの「脆弱性検索の方法」を参照してください。

手順

1. 次の手順に従って、脆弱性検索ツール (TMVS.exe) で製品名クエリの設定を指定します。
   a. TMVS.exe を起動します。
   b. [設定] をクリックします。
      [設定] 画面が表示されます。
   c. [製品名クエリ] セクションに移動します。
   d. チェックする製品を選択します。
   e. 製品名の横にある [設定] をクリックして、脆弱性検索ツールでチェックするポート番号を指定します。
   f. [OK] をクリックします。
      [設定] 画面が閉じます。
2. 脆弱性検索ツールがセキュリティソフトウェアを同時にチェックするコンピュータの数を設定するには、次の手順を実行します。
   a. <サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility¥TMVS に移動し、メモ帳などのテキストエディタを使用して TMVS.ini を開きます。
   b. 手動脆弱性検索でチェックするコンピュータの数を設定するには、ThreadNumManual の値を変更します。8～64 の値を指定します。

たとえば、同時に 60 台のコンピュータをチェックするには、「ThreadNumManual=60」と入力します。

c. 予約脆弱性検索でチェックするコンピュータの数を設定するには、ThreadNumSchedule の値を変更します。8～64 の値を指定します。

たとえば、同時に 50 台のコンピュータをチェックするには、「ThreadNumManual=50」と入力します。

d. TMVS.ini を保存します。

エンドポイントの説明を取得する方法

脆弱性検索ツールがホストコンピュータを「ping」できる場合、ホストコンピュータに関する追加情報を取得できます。情報を取得するには、次の 2 つの方法があります。

- クイック取得 (Quick):エンドポイント名のみを取得します。
- 標準取得 (Normal):ドメインとエンドポイントの両方の情報を取得します。

取得の設定

取得の設定は、脆弱性検索設定のサブセットです。脆弱性検索の設定の詳細については、172 ページの「脆弱性検索の方法」を参照してください。

手順

1. TMVS.exe を起動します。
2. [設定] をクリックします。

   [設定] 画面が表示されます。
3. [コンピュータの説明を取得する方法] セクションに移動します。
4. [標準] または [クイック] を選択します。
5. [標準] を選択した場合は、[可能な場合にコンピュータの説明を取得する] を選択します。

6. [OK] をクリックします。

   [設定] 画面が閉じます。

通知

脆弱性検索ツールでは、脆弱性検索結果を Apex One 管理者に送信できます。保護されていないホストコンピュータに通知を表示することもできます。

通知の設定

通知の設定は、脆弱性検索設定のサブセットです。脆弱性検索の設定の詳細については、172 ページの「脆弱性検索の方法」を参照してください。

手順

1. `TMVS.exe` を起動します。
2. [設定] をクリックします。

   [設定] 画面が表示されます。
3. [通知] セクションに移動します。
4. 脆弱性検索結果を自分自身または組織内の他の管理者に自動的に送信するには、次の手順を実行します。
   a. [結果をシステム管理者にメールで送信する] を選択します。
   b. [設定] をクリックして、メールの設定を指定します。
   c. [宛先] に、受信者のメールアドレスを入力します。
   d. [送信者] に、送信者のメールアドレスを入力します。
   e. [SMTP サーバ] に、SMTP サーバのアドレスを入力します。

      たとえば、「`smtp.company.com`」と入力します。SMTP サーバ情報が必要です。
   f. [件名] に、メッセージの新しい件名を入力するか、初期設定の件名をそのまま使用します。

g. [OK] をクリックします。

5. 使用しているコンピュータにセキュリティソフトウェアがインストールされていないことをユーザに通知するには、次の手順を実行します。

   a. [保護されていないコンピュータに通知を表示する] を選択します。

   b. [カスタマイズ] をクリックして、通知メッセージを設定します。

   c. [通知メッセージ] 画面で、新しいメッセージを入力するか、初期設定のメッセージをそのまま使用します。

   d. [OK] をクリックします。

6. [OK] をクリックします。

   [設定] 画面が閉じます。

脆弱性検索結果

脆弱性検索結果をカンマ区切り形式 (.csv) のファイルに保存するように脆弱性検索ツールを設定できます。

検索結果の設定

脆弱性検索結果の設定は、脆弱性検索設定のサブセットです。脆弱性検索の設定の詳細については、172 ページの「脆弱性検索の方法」を参照してください。

手順

1. `TMVS.exe` を起動します。
2. [設定] をクリックします。

   [設定] 画面が表示されます。
3. [結果の保存] セクションに移動します。
4. [CSV ファイルに結果を自動的に保存する] を選択します。
5. `.csv` ファイルを保存する初期設定のフォルダを変更するには、次の手順を実行します。

a. [参照] をクリックします。

b. エンドポイント上またはネットワーク上の保存先フォルダを選択します。

c. [OK] をクリックします。

6. [OK] をクリックします。

[設定] 画面が閉じます。

Ping 設定

対象コンピュータの有無を検証し、OS を特定するには、「ping」設定を使用します。これらの設定が無効な場合、脆弱性検索ツールは、いずれのホストコンピュータでも使用されていないものも含め、指定した IP アドレス範囲内のすべての IP アドレスを検索します。そのため、検索の試行に必要以上に時間がかかります。

Ping の設定

ping の設定は、脆弱性検索設定のサブセットです。脆弱性検索の設定の詳細については、172 ページの「脆弱性検索の方法」を参照してください。

手順

1. 次の手順に従って、脆弱性検索ツール (`TMVS.exe`) で ping の設定を指定します。

a. `TMVS.exe` を起動します。

b. [設定] をクリックします。

[設定] 画面が表示されます。

c. [Ping 設定] セクションに移動します。

d. [脆弱性検索ツールが ping でネットワークコンピュータのステータスを確認することを許可する] を選択します。

e. [パケットサイズ] フィールドおよび [タイムアウト] フィールドで、初期設定値をそのまま使用するか、変更します。

f. [ICMP OS フィンガープリント (ICMP エコーコード=19) を使用して OS タイプを検出する] を選択します。

このオプションを選択すると、ホストコンピュータで Windows が実行されているか、別の OS が実行されているかが脆弱性検索ツールによって確認されます。Windows を実行しているホストコンピュータについては、Windows のバージョンを特定できます。

g. [OK] をクリックします。

[設定] 画面が閉じます。

2. 脆弱性検索ツールが同時に ping するコンピュータの数を設定するには、次の手順を実行します。

a. <サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility¥TMVS に移動し、メモ帳などのテキストエディタを使用して TMVS.ini を開きます。

b. EchoNum の値を変更します。1～64 の値を指定します。

たとえば、同時に 60 台のコンピュータに ping コマンドを実行するようにするには、「EchoNum=60」と入力します。

c. TMVS.ini を保存します。

Apex One サーバの設定

Apex One サーバの設定は、次の場合に使用されます。

- 脆弱性検索ツールが、保護されていない対象コンピュータにセキュリティエージェントをインストールするとき。脆弱性検索ツールでは、サーバの設定を使用して、セキュリティエージェントの親サーバ、および対象コンピュータへのログオン時に使用する管理アカウント情報を特定できます。

注意

条件によっては、対象のホストコンピュータにセキュリティエージェントがインストールされない場合があります。

詳細については、171 ページの「脆弱性検索ツールを使用してセキュリティエージェントをインストールする際のガイドライン」を参照してください。

- 脆弱性検索ツールがエージェントインストールログを Apex One サーバに送信するとき。

Apex One サーバの設定

Apex One サーバの設定は、脆弱性検索設定のサブセットです。脆弱性検索の設定の詳細については、172 ページの「脆弱性検索の方法」を参照してください。

手順

1. `TMVS.exe` を起動します。
2. [設定] をクリックします。

   [設定] 画面が表示されます。
3. [Apex One サーバ設定] セクションに移動します。
4. Apex One サーバの名前とポート番号を入力します。
5. [保護されていないコンピュータにセキュリティエージェントを自動的にインストールする] を選択します。
6. 管理アカウント情報を設定するには、次の手順を実行します。
   a. [アカウントにインストール] をクリックします。
   b. [アカウント情報] 画面で、ユーザ名とパスワードを入力します。
   c. [OK] をクリックします。
7. [Apex One サーバにログを送信する] を選択します。
8. [OK] をクリックします。

[設定] 画面が閉じます。

セキュリティコンプライアンスを使用したインストール

ネットワークドメイン内のコンピュータにセキュリティエージェントをインストールするか、対象エンドポイントの IP アドレスを使用して対象エンドポイントにセキュリティエージェントをインストールします。

セキュリティエージェントをインストールする前に、次の点に注意してください。

手順

1. 各エンドポイントのログオン情報を記録しておきます。インストール時、Apex One によってこのログオン情報を指定するよう求められます。
2. 次の場合、エンドポイントにセキュリティエージェントはインストールされません。
   - エンドポイントに Apex One サーバがインストールされている。
   - エンドポイントで、Windows 7™ Starter、Windows 7 Home Basic、Windows 7 Home Premium、Windows 8.1 (通常版)、および Windows 10 Home が実行されている。これらのプラットフォームを実行しているエンドポイントでは、別のインストール方法を選択します。詳細については、144 ページの「配信時の注意事項」を参照してください。
3. 対象エンドポイントで Windows 7 (Professional、Enterprise、Ultimate Edition)、Windows 8.1 (Pro、Enterprise)、Windows 10 (Pro、Education、Enterprise)、Windows Server 2012 (Standard)、Windows Server 2016 (すべてのエディション)、または Windows Server 2019 (すべてのエディション) が実行されている場合は、そのエンドポイントで次の手順を実行します。
   a. ビルトインの管理者アカウントを有効にして、そのアカウントのパスワードを設定します。
   b. Windows のファイアウォールを無効にします。

c. [スタート] > [プログラム] > [管理ツール] > [セキュリティが強化された Windows ファイアウォール] の順にクリックします。

d. 「ドメイン プロファイル」、「プライベート プロファイル」、および「パブリック プロファイル」で、ファイアウォールの状態をオフにします。

e. Microsoft 管理コンソールを開いて ([スタート] > [ファイル名を指定して実行] の順にクリックして「`services.msc`」と入力)、Remote Registry サービスを開始します。セキュリティエージェントのインストール時には、ビルトインの管理者アカウントとパスワードを使用します。

4. トレンドマイクロまたはサードパーティのエンドポイントセキュリティプログラムがエンドポイントにインストールされている場合は、Apex One でそのソフトウェアを自動的にアンインストールしてからセキュリティエージェントに置き換えることが可能であるかどうかを確認します。Apex One で自動的にアンインストールされるエージェントセキュリティソフトウェアのリストについては、<サーバインストールフォルダ>¥PCCSRV¥Admin にある次のファイルを開いて確認してください。これらのファイルはメモ帳などのテキストエディタで開くことができます。

   - `tmuninst.ptn`
   - `tmuninst_as.ptn`

   対象エンドポイントのソフトウェアがリストに含まれていない場合は、そのソフトウェアを最初に手動でアンインストールします。ソフトウェアのアンインストール処理によっては、アンインストールの終了後、エンドポイントの再起動が必要になる場合があります。

セキュリティエージェントのインストール

手順

1. [診断] > [管理対象外のエンドポイント]に移動します。
2. エージェントツリーの上部で、[インストール] をクリックします。

- セキュリティエージェントの前のバージョンがエンドポイントにすでにインストールされている場合、[インストール] をクリックしても、Apex One でインストールはスキップされ、エージェントがこのバージョンにバージョンアップされません。エージェントをバージョンアップするには、次の設定を行います。

  a. [エージェント] > [エージェント管理] に移動します。

  b. [設定] > [権限とその他の設定] > [その他の設定] タブをクリックします。

  c. [アップデート設定] に移動します。

  d. [セキュリティエージェントがアップデートするコンポーネント] リストで、[すべてのコンポーネント (HotFix とエージェントプログラムを含む)] を選択します。

  e. [すべてのエージェントに適用] をクリックします。

3. エンドポイントごとに管理者のログオンアカウントを指定して、[ログオン] をクリックします。Apex One が対象エンドポイントへのエージェントのインストールを開始します。

4. インストールステータスを表示します。

他のウイルス対策ソフトからセキュリティエージェントへの移行

対象エンドポイントにインストールされているエージェントセキュリティソフトウェアを、セキュリティエージェントに置き換えます。

他のエンドポイントセキュリティソフトウェアからの移行

セキュリティエージェントをインストールするときに、インストールプログラムによって、トレンドマイクロまたはサードパーティのエンドポイントセキュリティソフトウェアが対象エンドポイントにインストールされているかどうかがチェックされます。インストールプログラムでは、ソフトウェアを

自動的にアンインストールし、セキュリティエージェントに置き換えることができます。

Apex One で自動的にアンインストールされるエンドポイントセキュリティソフトウェアのリストについては、<サーバインストールフォルダ>¥PCCSRV¥Admin にある次のファイルを開いて確認してください。メモ帳などのテキストエディタを使用して、これらのファイルを開きます。

- tmuninst.ptn
- tmuninst_as.ptn

対象エンドポイントのソフトウェアがリストに含まれていない場合は、そのソフトウェアを最初に手動でアンインストールします。ソフトウェアのアンインストール処理によっては、アンインストールの終了後、エンドポイントの再起動が必要になる場合があります。

セキュリティエージェントの移行の問題

- エージェントは自動的に移行されたが、インストールの直後にセキュリティエージェントで問題が発生した場合は、エンドポイントを再起動します。
- Apex One インストールプログラムでセキュリティエージェントのインストールを続行したが、他のセキュリティソフトウェアをアンインストールできなかった場合は、2 つのソフトウェアの間に競合が発生します。両方のソフトウェアをアンインストールしてから、144 ページの「配信時の注意事項」に記載されているインストール方法のいずれかを使用して、セキュリティエージェントをインストールします。

ServerProtect 一般サーバからの移行

ServerProtect 一般サーバ移行ツールを使用すると、ServerProtect 一般サーバが動作しているコンピュータをセキュリティエージェントに移行できます。

ServerProtect 一般サーバ移行ツールは、Apex One サーバと同じハードウェアとソフトウェアの仕様を共有します。Windows Server プラットフォームが動作しているコンピュータでツールを実行します。

ServerProtect 一般サーバのアンインストールが成功すると、ツールはセキュリティエージェントをインストールします。また、すべての検索タイプの検索除外リストの設定を、セキュリティエージェントに移行します。

セキュリティエージェントをインストール中に、移行ツールエージェントインストーラがタイムアウトになり、インストールが成功しなかったことが通知されることがありますが、セキュリティエージェントは正常にインストールされている場合があります。この場合、Apex One Web コンソールからセキュリティエージェントエンドポイントのインストールを確認してください。

次の状況では、移行は失敗します。

- リモートエージェントに IPv6 アドレスのみが割り当てられている。移行ツールでは IPv6 アドレス指定がサポートされていません。
- リモートエージェントが NetBIOS プロトコルを使用できない。
- ポート 455、337、および 339 がブロックされている。
- リモートエージェントが RPC プロトコルを使用できない。
- リモートレジストリサービスが停止している。

注意

ServerProtect 一般サーバ移行ツールでは、ServerProtect 用の Trend Micro Apex Central™エージェントはアンインストールされません。エージェントをアンインストールする方法については、ServerProtect または Apex Central のマニュアルを参照してください。

ServerProtect 一般サーバ移行ツールの使用

手順

1. Apex One サーバコンピュータで、<サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility¥SPNSXfr を開き、SPNSXfr.exe ファイルと SPNSX.ini ファイルを<サーバインストールフォルダ>¥PCCSRV¥Admin にコピーします。

2. SPNSXfr.exe をダブルクリックして、ツールを実行します。

   ServerProtect 一般サーバ移行ツールのコンソールが開きます。

3. Apex One サーバを選択します。Apex One サーバのパスが、Apex One サーバパスの下に表示されます。このパスが正しくない場合は、[選択] をクリックして、Apex One をインストールしたディレクトリの PCCSRV フォルダを選択します。次回ツールを開いたときに、Apex One サーバが再度自動的に検索されるようにするには、[自動検索サーバパス] チェックボックスをオンにします (初期設定ではオンになっています)。

4. [対象エンドポイント] で次のいずれかをクリックし、移行を実行する、ServerProtect 一般サーバが動作しているコンピュータを選択します。

   - Windows ネットワークツリー:ネットワークのドメインのツリーを表示します。この方法を使用してコンピュータを選択するには、エージェントコンピュータを検索するドメインをクリックします。
   - インフォメーションサーバ名:インフォメーションサーバ名で検索します。この方法でコンピュータを選択するには、テキストボックスにネットワーク上のインフォメーションサーバの名前を入力します。複数のインフォメーションサーバを検索するには、サーバ名の間にセミコロン「;」を挿入します。
   - 特定の一般サーバ名:一般サーバ名で検索します。この方法でコンピュータを選択するには、テキストボックスにネットワーク上の一般サーバの名前を入力します。複数の一般サーバを検索するには、サーバ名の間にセミコロン「;」を入力します。
   - IP アドレス範囲検索:IP アドレスの範囲で検索します。この方法でコンピュータを選択するには、IP 範囲でクラス B の IP アドレスの範囲を入力します。

   注意

   ネットワーク上の DNS サーバがエージェントの検索時に応答しない場合、検索は応答を停止します。検索がタイムアウトになるのを待ちます。

5. 移行後に対象コンピュータを自動的に再起動するには、[インストールした後に再起動します] を選択します。

移行を完了するには再起動が必要です。このオプションを選択しない場合は、移行後にコンピュータを手動で再起動してください。

6. [検索] をクリックします。

   検索結果が、ServerProtect 一般サーバの下に表示されます。

7. 移行を実行するコンピュータをクリックします。

   a. すべてのコンピュータを選択するには、[すべて選択] をクリックします。

   b. すべてのコンピュータの選択を解除するには、[すべて選択解除] をクリックします。

   c. リストをカンマ区切り形式 (.csv) のファイルにエクスポートするには、[CSV 形式ですべてエクスポート] をクリックします。

8. 対象コンピュータへのログインにユーザ名とパスワードが必要な場合は、次の操作を実行します。

   a. [グループアカウント/パスワードの使用] チェックボックスをオンにします。

   b. [ログオンアカウントの設定] をクリックします。

      [管理者情報の入力] ウィンドウが表示されます。

   c. ユーザ名とパスワードを入力します。

   注意

   ローカル/ドメイン管理者アカウントを使用して、対象エンドポイントにログオンします。「ゲスト」や「通常のユーザ」のような不十分な権限でログオンすると、インストールを実行できません。

   d. [OK] をクリックします。

   e. [ログオンに失敗した場合再度入力] をクリックすると、ログオンできなかった場合、移行処理中に再度ユーザ名とパスワードを入力できます。

9. [移行] をクリックします。

10. [インストールした後に再起動します] オプションを選択しなかった場合は、移行を完了するためにコンピュータを手動で再起動してください。

インストール後の確認

インストール完了後に、以下のことを確認してください。

- 196 ページの「プログラムのリスト」
- 196 ページの「セキュリティエージェントサービス」
- 197 ページの「セキュリティエージェントインストールログ」
- 198 ページの「推奨されるインストール後の確認タスク」

プログラムのリスト

エージェントエンドポイントのコントロールパネルで、[プログラムの追加と削除] に [Trend Micro Apex One セキュリティエージェント] が表示されます。

セキュリティエージェントサービス

Microsoft 管理コンソールに、次のセキュリティエージェントサービスが表示されます。

表 5-14. 初期設定のプロセス

プロセス名	説明	位置
TmListen.exe	Apex One サーバからコマンドと通知を受信して、セキュリティエージェントからサーバへの通信を制御します。	<エージェントのインストールフォルダ>\tmlisten.exe

プロセス名	説明	位置
NTRtScan.exe	セキュリティエージェントでリアルタイム検索、予約検索、および手動検索を実行します。	<エージェントのインストールフォルダ>\ntrtscan.exe
TmPfw.exe	パケットレベルファイアウォールおよびネットワークウイルス検索機能を提供します。	<エージェントのインストールフォルダ>\TmPfw.exe
TMBMSRV.exe	外部ストレージデバイスへのアクセスを規制し、レジストリキーおよびプロセスへの不正な変更を回避します。 注意 このオプションを有効にすると、エンドポイントへの他社製品のインストールがセキュリティエージェントによって阻止されることがあります。この問題が発生した場合は、このオプションを一時的に無効にして他社製品をインストールし、その後再びこのオプションを有効化してください。	<%Program Files (x86) フォルダ%>\Trend Micro\BM\TMBMSRV.exe
TmCCSF.exe	ブラウザ脆弱性対策およびメモリ検索を実行します。	<エージェントのインストールフォルダ>\CCSF\TmCCSF.exe
TmWSCSvc.exe	Apex One セキュリティエージェントのセキュリティステータスを Security Center に報告します。	<エージェントのインストールフォルダ>\TmWSCSvc.exe

セキュリティエージェントインストールログ

セキュリティエージェントインストールログ OFCNT.LOG は、以下の場所に格納されています。

- MSI パッケージインストールを除くすべてのインストール方法の場合は、%windir%

- MSI パッケージインストール方法の場合は、%temp%

推奨されるインストール後の確認タスク

以下のインストール後の確認タスクを実行することをお勧めします。

コンポーネントのアップデート

セキュリティ上の脅威に対してエージェントで最新の保護を実現するために、セキュリティエージェントコンポーネントをアップデートします。Web コンソールから手動エージェントアップデートを実行することも、各自のエンドポイントから「今すぐアップデート」を実行するようにユーザに指示することもできます。

EICAR テストスクリプトによるテスト検索

ヨーロッパコンピュータウイルス対策研究所 (EICAR) は、ウイルス対策ソフトウェアの適切なインストールと設定を確認する安全な方法として、EICAR テストスクリプトを開発しました。詳細については、次の EICAR Web サイトを参照してください。

http://www.eicar.org

EICAR テストスクリプトは.com 拡張子のある不活性なテキストファイルです。このスクリプトはウイルスではなく、ウイルスコードのフラグメントを含みませんが、大部分のウイルス対策ソフトウェアは、このスクリプトがウイルスであるかのように反応します。これを使用してウイルス感染をシミュレーションし、メール通知およびウイルスログが正常に機能することを確認します。

警告!

ウイルス対策製品のテストに、決して本物のウイルスを使用しないでください。

テスト検索の実行

手順

1. エージェントでリアルタイム検索を有効にします。
2. 次の文字列をコピーし、メモ帳やテキストエディタに貼り付けます。

   (実際の文字列では、改行は不要です。文字列中に改行があると検知されません。)

   ```
   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS
   -TEST-FILE!$H+H*
   ```

3. ファイルを `EICAR.com` として一時ディレクトリに保存します。Apex One がただちにファイルを検出します。
4. ネットワーク上の他のコンピュータをテストするには、EICAR.com ファイルをメールメッセージに添付し、ネットワーク上のコンピュータのいずれかに送信します。

> **ヒント**
>
> WinZip などの圧縮ソフトウェアを使用して EICAR ファイルをパッケージ化してから、別のテスト検索を実行することをお勧めします。

セキュリティエージェントのアンインストール

エンドポイントからセキュリティエージェントをアンインストールするには、次の 2 つの方法があります。

- 200 ページの「Web コンソールからのセキュリティエージェントのアンインストール」
- 202 ページの「セキュリティエージェントのアンインストールプログラムの実行」

Web コンソールからのセキュリティエージェントのアンインストール

セキュリティエージェントプログラムを Web コンソールからアンインストールします。プログラムで問題が発生した場合に限りアンインストールを実行し、その後ただちに再インストールして、セキュリティリスクからエンドポイントを保護します。

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [タスク] > [エージェントのアンインストール] の順にクリックします。
4. [エージェントのアンインストール] 画面で、[アンインストールの開始] をクリックします。
5. 通知のステータスをチェックし、通知を受信していないエージェントがあるかどうかを確認します。
   a. [未通知のエンドポイントを選択] > [アンインストールの開始] の順にクリックすると、未通知のエージェントに対してただちに通知が再送信されます。
   b. [アンインストールの中止] をクリックすると、現在通知されているエージェントへの通知を停止するように Apex One に指示します。すでに通知されたエージェントおよびアンインストールを実行しているエージェントは、このコマンドを無視します。

セキュリティエージェントのアンインストールプログラム

セキュリティエージェントのアンインストール権限を持つユーザは、ローカルエンドポイントのセキュリティエージェントプログラムをアンインストールできます。

設定によっては、アンインストールの際にパスワードが必要になることがあります。パスワードが必要な場合は、アンインストールプログラムを実行するユーザとのみパスワードを共有してください。パスワードが他のユーザに漏れた場合は、ただちにパスワードを変更してください。

セキュリティエージェントのアンインストール権限の付与

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [権限] タブの [アンインストール] セクションに移動します。
5. パスワードの要件を設定します。
   - パスワードを要求しない
   - パスワードを要求する: 必要なパスワードと確認用のパスワードを入力します。

   注意

   パスワードは以下の複雑さの要件を満たしている必要があります。
   - 8～32 文字の長さ
   - 大文字 (A～Z)、小文字 (a～z)、数字 (0～9)、特殊文字をそれぞれ 1 文字以上含む
   - 印刷できない ASCII 文字を含まない
6. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。

- すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
- 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

セキュリティエージェントのアンインストールプログラムの実行

手順

1. Windows の [スタート] メニューで、[プログラム] > [Trend Micro Apex One セキュリティエージェント] > [セキュリティエージェントのアンインストール] の順にクリックします。

   次の手順を実行することもできます。

   a. [コントロールパネル] > [プログラムのアンインストール] の順にクリックします。

   b. [Trend Micro Apex One セキュリティエージェント] を探し、[アンインストール] をクリックします。

   c. 画面の指示に従います。

2. アンインストールパスワードを要求された場合は入力します。アンインストールの進捗状況と完了が表示されます。

   注意

   エージェントに情報漏えい対策オプションをインストールした場合は、エンドポイントを再起動してアンインストールプロセスを完了する必要があります。

第 6 章

最新の保護状態の維持

この章では、Trend Micro Apex One のコンポーネントとアップデート手順について説明します。

この章は次のトピックで構成されます。

Apex One のコンポーネントとプログラム

Apex One では、最新のセキュリティリスクからエージェントエンドポイントを保護するために、さまざまなコンポーネントとプログラムを使用しています。これらのコンポーネントとプログラムを最新状態に保つには、手動アップデートまたは予約アップデートを実行します。

Apex One エージェントでは、コンポーネントだけでなく、アップデートされた設定ファイルを Apex One サーバから受け取ります。セキュリティエージェントで新しい設定を適用するには、設定ファイルが必要です。設定ファイルは、Web コンソールで Apex One 設定を変更するたびに変更されます。

コンポーネントは、次のグループに分けられます。

- 205 ページの「ウイルス対策コンポーネント」
- 208 ページの「スパイウェア対策コンポーネント」
- 209 ページの「ダメージクリーンナップサービスコンポーネント」
- 209 ページの「ファイアウォールコンポーネント」
- 210 ページの「挙動監視コンポーネント」
- 211 ページの「不審接続監視コンポーネント」
- 212 ページの「ブラウザ脆弱性対策」
- 212 ページの「プログラム」
- 214 ページの「Web レピュテーションコンポーネント」

ウイルス対策コンポーネント

コンポーネント	説明
ウイルス検索エンジン (32/64 ビット)	検索エンジンはウイルスおよび不正プログラムを検出するコンポーネントです。検索エンジンは高度な機能を備え、さまざまな種類のウイルスおよび不正プログラムを検出できます。 このエンジンとパターンファイルでは、すべてのファイルのすべてのバイトを検索するのではなく、連携することによって以下の特定を行います。 • ウイルスコードの手がかりとなる特性 • ウイルスが存在するファイル内の正確な位置
ウイルスパターンファイル	ウイルスパターンファイルには、最新のウイルス/不正プログラムおよび複合型脅威の攻撃をセキュリティエージェントが識別するための情報が格納されています。トレンドマイクロでは、週に数回、新バージョンのウイルスパターンファイルを作成し、リリースしているほか、特に破壊力のあるウイルス/不正プログラムの検出に伴い、随時、新バージョンのパターンファイルをリリースしています。
ウイルス検索ドライバ	ウイルス検索ドライバは、ファイルに対するユーザ操作を監視します。監視する操作としては、ファイルのオープン/クローズ、アプリケーションの実行などがあります。このドライバには 2 つのバージョンがあります。`TmXPFlt.sys` と `TmPreFlt.sys` です。`TmXPFlt.sys` はウイルス検索エンジンのリアルタイム設定に、`TmPreFlt.sys` はユーザによる操作の監視に使います。 **注意** このコンポーネントは、コンソールには表示されません。そのバージョンを確認するには、<サーバインストールフォルダ>¥PCCSRV¥Pccnt¥Drv に移動します。.sys ファイルを右クリックして、[プロパティ] を選択し、[バージョン情報] タブに移動します。

コンポーネント	説明
スマートスキャンパターンファイル スマートスキャンエージェントパターンファイル	スマートスキャンモードでは、セキュリティエージェントは 2 つの軽量型のパターンファイルを使用します。これらのパターンファイルは連携して、従来の不正プログラム対策およびウイルス対策パターンファイルにより提供されるものと同等の保護を提供します。 パターン定義の大部分はスマートスキャンパターンファイルに含まれています。スマートスキャンエージェントパターンファイルには、スマートスキャンパターンファイルに含まれないその他のすべてのパターン定義が含まれます。 セキュリティエージェントは、スマートスキャンエージェントパターンファイルを使用してセキュリティ上の脅威を検索します。検索時にファイルのリスクを特定できない場合、セキュリティエージェントは、Apex One サーバ上でホストされるサービスであるスキャンサーバに検索クエリを送信して、リスクを検証します。スキャンサーバは、スマートスキャンパターンファイルを使用してリスクを検証します。セキュリティエージェントは、検索のパフォーマンスを向上するために、スキャンサーバにより提供される検索クエリの結果を「キャッシュ」します。
IntelliTrap パターンファイル	IntelliTrap パターンファイルは、実行ファイルとして圧縮されたリアルタイム圧縮ファイルを検出します。 詳細については、828 ページの「IntelliTrap」を参照してください。
IntelliTrap 除外パターンファイル	IntelliTrap 除外パターンファイルには、「承認済み」圧縮ファイルのリストが含まれます。

コンポーネント	説明
メモリ検査パターンファイル	リアルタイム検索は、メモリ検査パターンファイルを使用して、挙動監視で検出された実行可能な圧縮ファイルを評価します。リアルタイム検索は、実行可能な圧縮ファイルに対して次の処理を実行します。 1. プロセスイメージパスの確認後、メモリ上にマッピングファイルを作成します。 **注意** 検索除外リストはファイル検索よりも優先されます。 2. プロセス ID を高度な保護サービスに送信します。高度な保護サービスでは次の処理が行われます。 a. ウイルス検索エンジンを使用してメモリ検索を実行します。 b. Windows システムファイル、信頼できるソースからのデジタル署名ファイル、およびトレンドマイクロでテスト済みのファイルのグローバルな承認済みリストを使用して、プロセスをフィルタします。一度安全が確認されたファイルに対して、Apex One ではそれ以降の処理は実行されません。 3. メモリ検索の処理後、高度な保護サービスはリアルタイム検索に結果を送信します。 4. リアルタイム検索は検出された不正プログラムを隔離し、プロセスを終了します。
CI エンジン (32/64 ビット)	CI エンジンは、あまり普及していないファイルで実行されるプロセスを監視し、動作の特性を抽出します。抽出された情報は、CI クエリハンドラによって、分析のために機械学習型検索エンジンに送信されます。
CI パターンファイル	CI パターンファイルには、既知のいずれの脅威にも関連しない「承認済み」の動作のリストが含まれます。
CI クエリハンドラ (32/64 ビット)	CI クエリハンドラは、CI エンジンで特定された動作を処理し、機械学習型検索エンジンにレポートを送信します。

コンポーネント	説明
高度な脅威検索エンジン (32/64 ビット)	高度な脅威検索エンジンは、あまり普及していないファイルからファイル特性を抽出し、その情報を機械学習型検索エンジンに送信します。
高度な脅威相関パターンファイル	高度な脅威相関パターンファイルには、既知のいずれの脅威にも関連しないファイル特性のリストが含まれます。

検索エンジンのアップデート

ウイルスパターンファイルに最も新しいウイルス/不正プログラムの情報を格納することで、セキュリティ対策の状態を最新に維持しながら、検索エンジンのアップデート数を最小限にとどめています。それにもかかわらず、定期的に新しい検索エンジンのバージョンが使用可能になります。トレンドマイクロは、次の状況で新しいエンジンを公開します。

- ソフトウェアへの新しい検索および検出テクノロジの導入
- 検索エンジンで処理できない、潜在的に有害な新しいウイルス/不正プログラムの検出
- 検索パフォーマンスの向上
- ファイル形式、スクリプト言語、エンコード、または圧縮形式の追加

スパイウェア対策コンポーネント

コンポーネント	説明
スパイウェア/グレーウェアパターンファイル	スパイウェアパターンファイルは、ファイル/プログラム、メモリ内のモジュール、Windows レジストリおよび URL ショートカット内のスパイウェア/グレーウェアを特定します。
スパイウェア検索エンジン (32/64 ビット)	スパイウェア検索エンジンは、スパイウェア/グレーウェアの検索を実行し、これらに適したスマートスキャンを実行します。

コンポーネント	説明
スパイウェア監視パターンファイル	スパイウェア監視パターンファイルは、スパイウェア/グレーウェアのリアルタイム検索に使用されます。エージェントはこのパターンファイルを、従来型スキャンでのみ使います。 スマートスキャンエージェントは、スパイウェア/グレーウェアのリアルタイム検索にスマートスキャンエージェントパターンファイルを使用します。検索時に検索対象のリスクを特定できない場合、エージェントは、スマートプロテクションソースに検索クエリを送信します。

ダメージクリーンナップサービスコンポーネント

コンポーネント	説明
ダメージクリーンナップエンジン (32 ビット/64 ビット)	ダメージクリーンナップエンジンはトロイの木馬およびトロイの木馬プロセスを検索して、除去します。
ダメージクリーンナップテンプレート	ダメージクリーンナップテンプレートは、ダメージクリーンナップエンジンでトロイの木馬ファイルとプロセスを特定し、削除するために使用されます。
起動時クリーンナップドライバ (32/64 ビット)	起動時クリーンナップドライバは、オペレーティングシステムのドライバ群より先にロードされ、ブート型ルートキットを検出、遮断します。セキュリティエージェントのロード後、起動時クリーンナップドライバはダメージクリーンナップサービスを呼び出して、ルートキットをクリーンナップします。

ファイアウォールコンポーネント

コンポーネント	説明
ファイアウォールドライバ (32/64 ビット)	ファイアウォールドライバは、ファイアウォールパターンファイルと併用して、ネットワークウイルスのエージェントのエンドポイントを検索するために使います。このドライバは 32 ビットおよび 64 ビットのプラットフォームに対応しています。

コンポーネント	説明
ファイアウォールパターンファイル	ウイルスパターンファイルと同様、ファイアウォールパターンファイルは、エージェントで、ウイルスシグネチャ (ネットワークウイルスの存在を示すビットやバイトの一意のパターン) の識別に使用されます。

挙動監視コンポーネント

コンポーネント	説明
挙動監視検出パターンファイル (32 ビット/64 ビット)	不審な脅威の挙動の検出に使用するルールが含まれるパターンファイルです。
挙動監視コアドライバ (32 ビット/64 ビット)	このカーネルモードドライバは、システムイベントを監視して、ポリシー施行のための挙動監視コアサービスに渡します。
挙動監視コアサービス (32 ビット/64 ビット)	このユーザモードサービスには、次の機能があります。 ・ ルートキット検出の提供 ・ 外部デバイスへのアクセス規制 ・ ファイル、レジストリキー、およびサービスの保護
挙動監視設定パターンファイル	挙動監視ドライバではこのパターンファイルを使用して通常のシステムイベントを識別し、それらをポリシー施行から除外します。
デジタル署名パターンファイル	このパターンファイルには、システムイベントを管理するプログラムが安全かどうかを特定するために挙動監視コアサービスで使用される、有効なデジタル署名のリストが含まれます。
ポリシー施行パターンファイル	挙動監視コアサービスでは、このパターンファイルのポリシーに照らしてシステムイベントがチェックされます。

コンポーネント	説明
メモリ検索実行パターンファイル (32 ビット/64 ビット)	挙動監視は、次の操作が実行されたことを検知すると、メモリ検索実行パターンファイルを使用して潜在的な脅威を特定します。 ・ ファイル書き込み処理 ・ レジストリ書き込み処理 ・ 新しいプロセスの作成 これらの操作のいずれかを検出すると、挙動監視は、リアルタイム検索のメモリ検査パターンファイルを呼び出してセキュリティリスクがあるかどうかをチェックします。 リアルタイム検索の詳細については、207 ページの「メモリ検査パターンファイル」を参照してください。
ダメージリカバリパターンファイル	ダメージリカバリパターンファイルには、不審な脅威の挙動監視に使用されるポリシーが含まれています。
プログラム検査監視パターンファイル	プログラム検査監視パターンファイルは、挙動監視に使用される検査ポイントを監視し、保存します。

不審接続監視コンポーネント

コンポーネント	説明
グローバル C&C IP リスト	グローバル C&C IP リストは、ネットワークコンテンツ検査エンジン (NCIE) が、既知の C&C サーバとのネットワーク接続を検出するために使います。NCIE は、C&C サーバとの、どのネットワークチャネルを介した接続でも検出できます。 Apex One は、グローバル C&C IP リストに載っているサーバに対する接続の情報をすべてログ出力し、評価できるようにします。
適合度ルールパターンファイル	不審接続監視サービスは、適合度ルールパターンファイルを使って、ネットワークパケットのヘッダを調べ、不正プログラムファミリに特有の署名を検出します。

ブラウザ脆弱性対策

コンポーネント	説明
ブラウザ脆弱性対策パターンファイル	このパターンファイルは、最新の Web ブラウザ脆弱性を識別し、脆弱性により Web ブラウザが悪用されることを防ぎます。
スクリプトアナライザ共通パターンファイル	このパターンファイルは、Web ページ内のスクリプトを分析し、不正なスクリプトを特定します。

プログラム

コンポーネント	説明
セキュリティエージェント	セキュリティエージェントプログラムは、セキュリティリスクからの実際の保護を提供します。
Basecamp	セキュリティを最適化してサポートを強化するために、トレンドマイクロでは Basecamp による基本的なエンドポイント情報の定期的な収集を許可することを推奨します。 重要 Basecamp からトレンドマイクロへのデータの送信を開始する前に、データの収集に同意する必要があります。 Basecamp を使用するにはインターネットに接続する必要があるため、ファイアウォールに関する追加の設定が必要になる場合があります。 • ファイル名: `EndpointBasecamp.exe` • インストールパス: `C:¥Program Files¥Trend Micro ¥Endpoint Basecamp`

コンポーネント	説明
HotFix、Patch、および Service Pack	製品の正式リリース後、トレンドマイクロでは、問題への対処、製品のパフォーマンスの強化、または新機能の追加のために次のものを開発しています。 • 827 ページの「HotFix」 • 831 ページの「Patch」 • 833 ページの「Critical Patch」 • 833 ページの「Service Pack」 下記のトレンドマイクロの Web サイトで、新しい Critical Patch、Patch、または Service Pack のリリースに関する情報を確認してください。 http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp すべてのリリースには、インストール、配信、および設定に必要な情報が記載された Readme ファイルが含まれています。Readme ファイルをよくお読みのうえ、インストールしてください。

HotFix と Patch の履歴

Apex One サーバが HotFix や Patch ファイルをセキュリティエージェントに配信すると、エージェントプログラムでは、レジストリエディタに HotFix と Patch に関する情報が記録されます。Microsoft SMS、LANDesk、BigFix などのロジスティクスソフトウェアを使用して、複数のエージェントに対してこの情報を照会できます。

注意

この機能では、サーバにのみ配信された HotFix や Patch は記録されません。

情報は、次のキーに格納されます。

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\HotfixHistory\<製品バージョン>`
- x64 タイプのプラットフォームを実行するコンピュータの場合:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\ PC-
cillinNTCorp\CurrentVersion\HotfixHistory\<製品バージョン>
```

次のキーを確認してください。

- キー: `HotFix_installed`

  種類: `REG_SZ`

  値:`<HotFix または Patch 名>`

- キー: `HotfixInstalledNum`

  種類: `DWORD`

  値: `<HotFix または Patch 番号>`

Web レピュテーションコンポーネント

コンポーネント	説明
URL フィルタエンジン	URL フィルタエンジンは、Apex One と URL フィルタサービスとの通信を担います。URL フィルタサービスは、URL を査定 (レーティング) し、その情報を Apex One に渡すシステムです。

アップデートの概要

すべてのコンポーネントのアップデートは、トレンドマイクロのアップデートサーバから取得されます。新しいコンポーネントが入手可能になると、Apex One サーバおよび Trend Micro Smart Protection ソース (Smart Protection Server または Trend Micro Smart Protection Network) は、アップデートされたコンポーネントをダウンロードします。Apex One サーバと Trend Micro Smart Protection ソースの間でダウンロードするコンポーネントが重複することはありません。これは、それぞれが固有のコンポーネントセットをダウンロードするためです。

注意

Apex One サーバと Smart Protection Server は両方とも、トレンドマイクロのアップデートサーバ以外のアップデート元からアップデートするように設定できます。これを行うには、ユーザ指定のアップデート元を設定する必要があります。アップデート元の設定について支援が必要な場合には、サポートセンターまでお問い合わせください。

Apex One サーバとセキュリティエージェントのアップデート

Apex One サーバは、エージェントに必要な大半のコンポーネントをダウンロードします。ダウンロードしない唯一のコンポーネントは、Trend Micro Smart Protection ソースによってダウンロードされるスマートスキャンパターンファイルです。

Apex One サーバが多数のエージェントを管理している場合、アップデートに大量のサーバコンピュータリソースが使用される場合があり、サーバの安定性とパフォーマンスに影響する可能性があります。この問題に対応するために、Apex One にはアップデートエージェント機能が用意されています。この機能により、特定の複数のエージェントが、他のエージェントにアップデートを配信するタスクを共有することができます。

次の表は、Apex One サーバおよびエージェントに対するさまざまなコンポーネントアップデートのオプションと、これらを使用する際の推奨事項について説明しています。

表 6-1. サーバとエージェントのアップデートオプション

アップデートオプション	説明	推奨事項
[トレンドマイクロのアップデートサーバ] > サーバ > エージェント	Apex One サーバは、アップデートされたコンポーネントをトレンドマイクロのアップデートサーバ (またはその他のアップデート元) から受信し、エージェントでコンポーネントのアップデートを開始します。	Apex One サーバとエージェントの間に低帯域幅のセグメントがない場合、この方法を使用します。

アップデートオプション	説明	推奨事項
[トレンドマイクロのアップデートサーバ] > サーバ > [アップデートエージェント] > エージェント	Apex One サーバが、アップデートされたコンポーネントをトレンドマイクロのアップデートサーバ (またはその他のアップデート元) から受信し、エージェントでコンポーネントのアップデートを開始します。次に、アップデートエージェントとして機能するエージェントが、エージェントにコンポーネントをアップデートするように通知します。	Apex One サーバとエージェントの間に低帯域幅のセグメントがある場合、ネットワークのトラフィック負荷を分散するためにこの方法を使用します。
[トレンドマイクロのアップデートサーバ] > [アップデートエージェント] > エージェント	アップデートエージェントが、アップデートされたコンポーネントをトレンドマイクロのアップデートサーバ (またはその他のアップデート元) から直接受信し、エージェントにコンポーネントをアップデートするように通知します。	アップデートエージェントを Apex One サーバまたは他のアップデートエージェントからアップデートする際に問題が発生する場合にのみ、この方法を使用します。 ほとんどの環境では、アップデートエージェントは、外部のアップデート元からよりも、Apex One サーバまたは他のアップデートエージェントからの方がアップデートを速く受信できます。
[トレンドマイクロのアップデートサーバ] > エージェント	Apex One エージェントが、アップデートされたコンポーネントをトレンドマイクロのアップデートサーバ (またはその他のアップデート元) から直接受信します。	エージェントを Apex One サーバまたはアップデートエージェントからアップデートする際に問題が発生する場合にのみ、この方法を使用します。 ほとんどの環境では、エージェントは、外部のアップデート元からよりも、Apex One サーバまたはアップデートエージェントからの方がアップデートを速く受信できます。

Trend Micro Smart Protection ソースのアップデート

スマートスキャンパターンファイルは、Trend Micro Smart Protection ソース (Smart Protection Server または Trend Micro Smart Protection Network) によって、ダウンロードされます。スマートスキャンエージェントでは、このパターンファイルはダウンロードされません。エージェントから Trend Micro Smart Protection ソースに検索クエリを送信し、パターンファイルに照らして潜在的脅威を検証します。

注意

Trend Micro Smart Protection ソースの詳細については、106 ページの「Trend Micro Smart Protection ソース」を参照してください。

次の表は、Trend Micro Smart Protection ソースのアップデート処理について説明しています。

表 6-2. Trend Micro Smart Protection ソースのアップデート処理

アップデート処理	説明
[トレンドマイクロのアップデートサーバ] > [Smart Protection Network]	Trend Micro Smart Protection Network は、トレンドマイクロのアップデートサーバからアップデートを受信します。企業ネットワークに接続されていないスマートスキャンエージェントは、Trend Micro Smart Protection Network にクエリを送信します。
[トレンドマイクロのアップデートサーバ] > [Smart Protection Server]	Smart Protection Server (統合またはスタンドアロン) は、トレンドマイクロのアップデートサーバからアップデートを受信します。企業ネットワークに接続されている Trend Micro Smart Protection エージェントは、Smart Protection Server にクエリを送信します。
[Smart Protection Network] > [Smart Protection Server]	Smart Protection Server (統合またはスタンドアロン) は、Trend Micro Smart Protection Network からアップデートを受信します。企業ネットワークに接続されている Trend Micro Smart Protection エージェントは、Smart Protection Server にクエリを送信します。

Apex One サーバのアップデート

Apex One サーバは、次のコンポーネントをダウンロードして、エージェントに配信します。

表 6-3. Apex One サーバがダウンロード可能なコンポーネント

コンポーネント	配信	
	従来型スキャンエージェント	スマートスキャンエージェント
ウイルス対策		
スマートスキャンエージェントパターンファイル	なし	あり
ウイルスパターンファイル	あり	なし
IntelliTrap パターンファイル	あり	あり
IntelliTrap 除外パターンファイル	あり	あり
ウイルス検索エンジン (32/64 ビット)	あり	あり
メモリ検査パターンファイル	あり	あり
ELAM パターンファイル (32/64 ビット)	あり	あり
CI エンジン (32/64 ビット)	あり	あり
CI パターンファイル	あり	あり
CI クエリハンドラ (32/64 ビット)	あり	あり
高度な脅威検索エンジン (32/64 ビット)	あり	あり
高度な脅威相関パターンファイル	あり	あり
スパイウェア対策		
スパイウェア/グレーウェアパターンファイル	あり	あり
スパイウェア監視パターンファイル	あり	なし

コンポーネント	配信	
	従来型スキャンエージェント	スマートスキャンエージェント
スパイウェア検索エンジン (32/64 ビット)	あり	あり
ダメージクリーンナップサービス		
ダメージクリーンナップテンプレート	あり	あり
ダメージクリーンナップエンジン (32 ビット/64 ビット)	あり	あり
起動時クリーンナップドライバ (32/64 ビット)	あり	あり
ファイアウォール		
ファイアウォールパターンファイル	あり	あり
挙動監視コンポーネント		
挙動監視検出パターンファイル (32 ビット/64 ビット)	あり	あり
挙動監視コアドライバ (32 ビット/64 ビット)	あり	あり
挙動監視コアサービス (32 ビット/64 ビット)	あり	あり
挙動監視設定パターンファイル	あり	あり
ポリシー施行パターンファイル	あり	あり
デジタル署名パターンファイル	あり	あり
メモリ検索実行パターンファイル (32 ビット/64 ビット)	あり	あり
プログラム検査監視パターンファイル	あり	あり
ダメージリカバリパターンファイル	あり	あり
不審接続監視		

コンポーネント	配信	
	従来型スキャンエージェント	スマートスキャンエージェント
グローバル C&C IP リスト	あり	あり
適合度ルールパターンファイル	あり	あり
ブラウザ脆弱性対策		
ブラウザ脆弱性対策パターンファイル	あり	あり
スクリプトアナライザ共通パターンファイル	あり	あり

アップデートに関する注意事項とヒント:

- アップデートされたコンポーネントをサーバからエージェントに配信できるようにするには、エージェントの自動アップデートを有効にします。詳細については、242 ページの「セキュリティエージェントの自動アップデート」を参照してください。エージェントの自動アップデートが無効な場合でも、サーバはアップデートをダウンロードしますが、エージェントに配信することはありません。
- IPv6 シングルスタックの Apex One サーバから IPv4 シングルスタックエージェントには、アップデートを直接配信することができません。同様に、IPv4 シングルスタックの Apex One サーバから IPv6 シングルスタックエージェントにも、アップデートを直接配信することができません。このような場合に、Apex One サーバからエージェントにアップデートを配信するには、IP アドレス変換が可能な DeleGate などのデュアルスタックプロキシサーバが必要です。
- トレンドマイクロでは、定期的にパターンファイルをリリースして、エージェントの保護を最新状態に維持しています。パターンファイルのアップデートは定期的に入手可能になるので、Apex One では「コンポーネントの複製」というメカニズムを使用して、パターンファイルの高速なダウンロードを実現しています。詳細については、223 ページの「Apex One サーバコンポーネントの複製」を参照してください。
- プロキシサーバを使用してインターネットに接続している場合、アップデートを正常にダウンロードするように正しいプロキシ設定を使用してください。

- Web コンソールのダッシュボードで、エージェントのアップデート状況ウィジェットを追加し、コンポーネントの現在のバージョンを表示し、コンポーネントがアップデートされているエージェントの数と、古いままのエージェントの数を確認します。

Apex One サーバのアップデート元

トレンドマイクロのアップデートサーバまたは他のアップデート元からコンポーネントをダウンロードするように、Apex One サーバを設定します。Apex One サーバから直接トレンドマイクロのアップデートサーバに接続できない場合は、別のアップデート元を指定できます。サンプルシナリオについては、226 ページの「隔離された Apex One サーバのアップデート」を参照してください。

サーバは、使用可能なアップデートをダウンロードすると、[アップデート] > [エージェント] > [自動アップデート]で指定された設定に基づいて、エージェントにコンポーネントをアップデートするように自動的に通知できます。コンポーネントのアップデートが重要な場合は、[アップデート] > [エージェント] > [手動アップデート]に進んで、エージェントに一度に通知するようにサーバを設定できます。

注意

[アップデート] > [エージェント] > [自動アップデート]で、配信スケジュールや、イベント起動配信の設定を指定していない場合には、サーバがアップデートをダウンロードしても、エージェントへのアップデートの通知は実行されません。

Apex One サーバアップデートでの IPv6 のサポート

IPv6 シングルスタックの Apex One サーバを、次のような IPv4 シングルスタックのアップデート元から直接アップデートすることはできません。

- トレンドマイクロのアップデートサーバ
- IPv4 シングルスタックのユーザ指定のアップデート元

同様に、IPv4 シングルスタックの Apex One サーバを、IPv6 シングルスタックのユーザ指定のアップデート元から直接アップデートすることはできません。

このようなサーバがアップデート元に接続できるようにするには、IP アドレスを変換可能な DeleGate などのデュアルスタックプロキシサーバが必要です。

Apex One サーバアップデートのプロキシ

トレンドマイクロのアップデートサーバからアップデートをダウンロードするときにプロキシ設定を使用するように、サーバコンピュータでホストされたサーバプログラムを設定します。サーバプログラムには、Apex One サーバと統合 Smart Protection Server があります。

サーバのプロキシ設定

手順

1. [管理] > [設定] > [プロキシ] に移動します。
2. [サーバ] タブを選択します。
3. [トレンドマイクロのサーバに接続してパターンファイル、エンジン、およびライセンスをアップデートする際に、次のプロキシ設定を使用する] を選択します。
4. プロキシプロトコル、サーバ名または IPv4/IPv6 アドレス、およびポート番号を指定します。
5. プロキシサーバで認証が必要な場合は、ユーザ名とパスワードを入力します。
6. [保存] をクリックします。

サーバアップデート元の設定

手順

1. [アップデート] > [サーバ] > [アップデート元] に移動します。

2. コンポーネントのアップデートのダウンロード元になる場所を選択します。

   トレンドマイクロのアップデートサーバを選択する場合は、サーバがインターネットに接続されていることを確認し、プロキシサーバを使用している場合は、プロキシ設定を使用してインターネット接続が可能かどうかをテストしてください。詳細については、222 ページの「Apex One サーバアップデートのプロキシ」を参照してください。

   ユーザ指定のアップデート元を選択する場合は、適切な環境を設定して、このアップデート元のリソースをアップデートしてください。また、サーバコンピュータとこのアップデート元との接続が機能することも確認してください。アップデート元の設定について支援が必要な場合には、サポートセンターまでお問い合わせください。

   注意

   Apex One サーバは、アップデート元からコンポーネントをダウンロードするときに、コンポーネントの複製を使用します。詳細については、223 ページの「Apex One サーバコンポーネントの複製」を参照してください。

3. [保存] をクリックします。

Apex One サーバコンポーネントの複製

トレンドマイクロのアップデートサーバからのダウンロード用に、最新バージョンの完全なパターンファイルが入手可能になったときには、14 個の「差分パターンファイル」も入手可能になります。差分パターンファイルは、完全なパターンファイルよりもサイズが小さなバージョンで、以前の完全なパターンファイルと最新バージョンの差分に相当します。たとえば、最新バージョンが 175 の場合、差分パターンファイル v_173.175 には、バージョン 173 に存在しないバージョン 175 のシグネチャが含まれています。パターンファイル番号は 2 ずつ増やされるため、バージョン 173 は前の完全なパターンファイルのバージョンです。差分パターンファイル v_171.175 には、バージョン 171 に存在しないバージョン 175 のシグネチャが含まれています。

Apex One では、最新パターンファイルをダウンロードするときに生じるネットワークトラフィックを軽減するために、コンポーネントの複製が実行されます。これは、Apex One サーバまたはアップデートエージェントが差分パ

ターンファイルのみをダウンロードするコンポーネントのアップデート方法です。アップデートエージェントがコンポーネントの複製を実行する方法については、265 ページの「アップデートエージェントのコンポーネントの複製」を参照してください。

コンポーネントの複製は、次のコンポーネントに適用されます。

- ウイルスパターンファイル
- スマートスキャンエージェントパターンファイル
- ダメージクリーンナップテンプレート
- IntelliTrap 除外パターンファイル
- スパイウェア/グレーウェアパターンファイル
- スパイウェア監視パターンファイル

コンポーネントの複製のシナリオ

サーバのコンポーネントの複製については、次のシナリオを参照してください。

表 6-4. サーバコンポーネントの複製のシナリオ

Apex One サーバのフルパターンファイル	**現在のバージョン:** 171 **利用可能なその他のバージョン:** 169	167	165	161	159	
トレンドマイクロのアップデートサーバの最新バージョン	173.175	171.175	169.175	167.175	165.175	163.175
	161.175	159.175	157.175	155.175	153.175	151.175
	149.175	147.175				

1. Apex One サーバは、現在のフルパターンファイルのバージョンと、トレンドマイクロのアップデートサーバの最新バージョンを比較します。2 つのバージョンの差が 14 以下の場合、サーバは、2 つのバージョンの差分に相当する差分パターンファイルのみをダウンロードします。

注意

差が 14 を超える場合、サーバは自動的にフルパターンファイルと、14 個の差分パターンファイルをダウンロードします。

実際の例では次のようになります。

- バージョン 171 と 175 の差は 2 です。つまり、サーバにはバージョン 173 と 175 がありません。
- このサーバは、差分パターンファイル 171.175 をダウンロードします。この差分パターンファイルは、バージョン 171 と 175 の差分に相当します。

2. サーバで差分パターンファイルと現在の完全なパターンファイルが結合されて、最新の完全なパターンファイルが生成されます。

   実際の例では次のようになります。

   - サーバで、Apex One がバージョン 171 と差分パターンファイル 171.175 を結合して、バージョン 175 を生成します。
   - このサーバには、1 つの差分パターンファイル (171.175) と、最新の完全なパターンファイル (バージョン 175) が存在します。

3. サーバでは、サーバ上にある他の完全なパターンファイルに基づいて、差分パターンファイルが生成されます。サーバがこれらの差分パターンを生成しない場合、以前の差分パターンのダウンロードに失敗したエージェントは自動的にフルパターンファイルをダウンロードします。これによって、結果的により多くのネットワークトラフィックが生じます。

   実際の例では次のようになります。

   - サーバには、169、167、165、163、161、159 のパターンファイルバージョンがあるため、次の差分パターンファイルを生成できます。

     169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - このサーバには差分パターンファイル 171.175 がすでにあるため、バージョン 171 を使用する必要はありません。
   - 現在サーバには、次の 7 つの差分パターンファイルが存在します。

     171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

- このサーバでは、最近の 7 つの完全なパターンファイルバージョン (バージョン 175、171、169、167、165、163、161) が保持されます。これよりも古いバージョン (バージョン 159) は削除されます。

4. サーバで、現在の差分パターンファイルと、トレンドマイクロのアップデートサーバにある差分パターンファイルが比較されます。サーバにない、差分パターンファイルがダウンロードされます。

   実際の例では次のようになります。

   - トレンドマイクロのアップデートサーバには、次の 14 個の差分パターンファイルが存在します。

     173.175, 171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

   - Apex One サーバには、次の 7 つの差分パターンファイルが存在します。

     171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - Apex One サーバは、追加として次の 7 つの差分パターンファイルをダウンロードします。

     173.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

   - これで、トレンドマイクロのアップデートサーバにあるすべての差分パターンファイルが、このサーバに存在することになります。

5. 最新のフルパターンファイルと 14 個の差分パターンファイルが、エージェントから使用可能になります。

隔離された Apex One サーバのアップデート

ここでは隔離された Apex One サーバのアップデートについて説明します。

隔離された Apex One サーバのアップデート手順

Apex One サーバが外部ソースと完全に隔離されたネットワークに存在している場合、次の製品 Q&A にある手順でサーバのコンポーネントを最新の状態に保持できます。https://success.trendmicro.com/jp/solution/1308958

Apex One サーバが [アップデート元] には接続できる場合、以下手順でサーバのコンポーネントを最新の状態に保持できます。

手順

1. Trend Micro Apex Central やランダムホストコンピュータなどのアップデート元を特定します。アップデート元の要件は次のとおりです。
   - トレンドマイクロのアップデートサーバから最新コンポーネントをダウンロードすることが可能な安全なインターネット接続があること。
   - Apex One サーバとの接続が機能していること。Apex One サーバとアップデート元間にプロキシサーバがある場合は、プロキシ設定を行います。詳細については、222 ページの「Apex One サーバアップデートのプロキシ」を参照してください。
   - ディスクの空き容量が十分にあり、ダウンロードしたコンポーネントを格納できること。
2. Apex One サーバで、新しいアップデート元を指定します。詳細については、221 ページの「Apex One サーバのアップデート元」を参照してください。
3. サーバからエージェントに配信されるコンポーネントを特定します。配信可能なコンポーネントのリストについては、231 ページの「セキュリティエージェントのアップデート」を参照してください。

   ヒント

   エージェントにコンポーネントが配信中かどうかを確認する方法の 1 つに、Web コンソールの [アップデートの概要] 画面 ([アップデート] > [概要]) を表示する方法があります。この画面で、配信対象のコンポーネントのアップデート率は必ず 0%より大きくなります。
4. コンポーネントのダウンロード頻度を決定します。パターンファイルは更新頻度が高いため (一部は毎日)、定期的にアップデートすることをお勧めします。
5. アップデート元で次の手順を実行します。

a. トレンドマイクロのアップデートサーバに接続します。サーバの URL は、ご使用の Apex One のバージョンによって異なります。

b. 次の項目をダウンロードします。

- `server.ini` ファイル。このファイルには、最新のコンポーネントに関する情報が含まれています。
- 手順 3 で特定したコンポーネント。

c. ダウンロードしたアイテムを、アップデート元のディレクトリに保存します。

6. Apex One サーバの手動アップデートを実行します。詳細については、229 ページの「Apex One サーバの手動アップデート」を参照してください。

7. コンポーネントのアップデートが必要になるたびに手順 5～6 を繰り返します。

Apex One サーバのアップデート方法

Apex One サーバのコンポーネントのアップデートは、手動で行うか、またはアップデートスケジュールを設定することによって行います。

アップデートされたコンポーネントをサーバからエージェントに配信できるようにするには、エージェントの自動アップデートを有効にします。詳細については、242 ページの「セキュリティエージェントの自動アップデート」を参照してください。エージェントの自動アップデートが無効の場合でも、サーバはアップデートをダウンロードしますが、エージェントに配信することはありません。

アップデートには次の方法があります。

- 手動サーバアップデート:重要なアップデートがある場合には、手動アップデートを実行することによりサーバでただちにアップデートを取得できます。詳細については、229 ページの「Apex One サーバの手動アップデート」を参照してください。
- 予約サーバアップデート:Apex One サーバは、予約された日時にアップデート元に接続して、最新のコンポーネントを取得します。詳細につい

ては、229 ページの「Apex One サーバのアップデートの予約」を参照してください。

Apex One サーバの手動アップデート

サーバをインストールまたはバージョンアップした後、および大規模感染が発生したときには、Apex One サーバでコンポーネントを手動でアップデートします。

手順

1. [アップデート] > [サーバ] > [手動アップデート] に移動します。
2. アップデート対象コンポーネントを選択します。
3. [アップデート] をクリックします。

   サーバがアップデートされたコンポーネントをダウンロードします。

Apex One サーバのアップデートの予約

定期的にアップデート元をチェックして、利用可能なアップデートを自動的にダウンロードするように、Apex One サーバを設定します。エージェントは通常、サーバからアップデートを取得するため、予約アップデートを使用することは、セキュリティリスクに対する保護を常に最新に維持する簡単かつ効率的な方法となります。

手順

1. [アップデート] > [サーバ] > [予約アップデート]に移動します。
2. [Apex One サーバの予約アップデートを有効にする] を選択します。
3. アップデート対象コンポーネントを選択します。
4. アップデートスケジュールを指定します。

   アップデートスケジュールで、毎日、毎週、毎月を選択した場合、アップデートを実行する期間を時間単位で指定します。Apex One は、この期間中の任意の時間にアップデートを実行します。

5. [保存]をクリックします。

Apex One サーバのアップデートログ

特定のコンポーネントをアップデートする際に問題が発生するかどうかを判断するには、サーバアップデートログを確認します。ログには、Apex One サーバのコンポーネントのアップデートについて記録されています。

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログの削除スケジュールを設定します。ログの管理方法の詳細については、616 ページの「ログ管理」を参照してください。

アップデートログの表示

手順

1. [ログ] > [サーバアップデート] に移動します。
2. [結果] 列で、アップデートされていないコンポーネントがあるかどうかを確認します。
3. ログを CSV ファイルに保存するには、[CSV 形式ですべてエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。

統合 Smart Protection Server のアップデート

統合 Smart Protection Server は、スマートスキャンパターンファイルと Web ブロックリストの 2 つのコンポーネントをダウンロードします。これらのコンポーネントの詳細とアップデート方法については、119 ページの「統合 Smart Protection Server の管理」を参照してください。

セキュリティエージェントのアップデート

最新のセキュリティリスクに対するエージェントの保護状態を維持するには、エージェントのコンポーネントを定期的にアップデートします。

エージェントをアップデートする前に、アップデート元 (Apex One サーバまたはユーザ指定のアップデート元) に最新のコンポーネントがあるかどうかを確認してください。Apex One サーバのアップデート方法については、218 ページの「Apex One サーバのアップデート」を参照してください。

次の表は、アップデート元がエージェントに配信するコンポーネントと、特定の検索方法で使用されるすべてのコンポーネントを示しています。

表 6-5. エージェントに配信される Apex One コンポーネント

コンポーネント	配信	
	従来型スキャンエージェント	スマートスキャンエージェント
ウイルス対策		
スマートスキャンエージェントパターンファイル	なし	あり
ウイルスパターンファイル	あり	なし
IntelliTrap パターンファイル	あり	あり
IntelliTrap 除外パターンファイル	あり	あり
ウイルス検索エンジン (32/64 ビット)	あり	あり
メモリ検査パターンファイル	あり	あり
ELAM パターンファイル (32/64 ビット)	あり	あり
CI エンジン (32/64 ビット)	あり	あり
CI パターンファイル	あり	あり
CI クエリハンドラ (32/64 ビット)	あり	あり
高度な脅威検索エンジン (32/64 ビット)	あり	あり

コンポーネント	配信	
	従来型スキャンエージェント	スマートスキャンエージェント
高度な脅威相関パターンファイル	あり	あり
スパイウェア対策		
スパイウェア/グレーウェアパターンファイル	あり	あり
スパイウェア監視パターンファイル	あり	なし
スパイウェア検索エンジン (32/64 ビット)	あり	あり
ダメージクリーンナップサービス		
ダメージクリーンナップテンプレート	あり	あり
ダメージクリーンナップエンジン (32 ビット/64 ビット)	あり	あり
起動時クリーンナップドライバ (32/64 ビット)	あり	あり
Web レピュテーションサービス		
URL フィルタエンジン	あり	あり
ファイアウォール		
ファイアウォールパターンファイル	あり	あり
ファイアウォールドライバ (32/64 ビット)	あり	あり
挙動監視コンポーネント		
挙動監視検出パターンファイル (32 ビット/64 ビット)	あり	あり
挙動監視コアドライバ (32 ビット/64 ビット)	あり	あり

コンポーネント	配信	
	従来型スキャンエージェント	スマートスキャンエージェント
挙動監視コアサービス (32 ビット/64 ビット)	あり	あり
挙動監視設定パターンファイル	あり	あり
ポリシー施行パターンファイル	あり	あり
デジタル署名パターンファイル	あり	あり
メモリ検索実行パターンファイル (32 ビット/64 ビット)	あり	あり
プログラム検査監視パターンファイル	あり	あり
ダメージリカバリパターンファイル	あり	あり
不審接続監視		
グローバル C&C IP リスト	あり	あり
適合度ルールパターンファイル	あり	あり
ブラウザ脆弱性対策		
ブラウザ脆弱性対策パターンファイル	あり	あり
スクリプトアナライザ共通パターンファイル	あり	あり

セキュリティエージェントのアップデート元

エージェントは、標準のアップデート元 (Apex One サーバ) からアップデートを取得するか、トレンドマイクロのアップデートサーバなどのユーザ指定のアップデート元から特定コンポーネントを取得することができます。詳細については、234 ページの「セキュリティエージェントの標準のアップデート元」および 236 ページの「セキュリティエージェントのユーザ指定のアップデート元」を参照してください。

セキュリティエージェントアップデートでの IPv6 のサポート

IPv6 シングルスタックエージェントを、次のような IPv4 シングルスタックのアップデート元から直接アップデートすることはできません。

- IPv4 シングルスタックの Apex One サーバ
- IPv4 シングルスタックのアップデートエージェント
- IPv4 シングルスタックのユーザ指定のアップデート元
- トレンドマイクロのアップデートサーバ

同様に、IPv4 シングルスタックエージェントを、IPv6 シングルスタックの Apex One サーバやアップデートエージェントなど、IPv6 シングルスタックのアップデート元から直接アップデートすることはできません。

エージェントがこれらのアップデート元に接続するには、DeleGate など、IP アドレスを変換できるデュアルスタックプロキシサーバが必要です。

セキュリティエージェントの標準のアップデート元

Apex One サーバは、エージェントの標準のアップデート元です。

Apex One サーバが接続不能で、その他のアップデート元も使用できない場合は、エージェントは古い状態のままになります。Apex One サーバに接続できないエージェントをアップデートするには、エージェントパッケージャの使用をお勧めします。このツールを使用して、サーバで提供可能な最新コンポーネントのパッケージを作成し、エージェントでこのパッケージを実行します。

注意

エージェントの IP アドレス (IPv4 または IPv6) によって、Apex One サーバへの接続を確立できるかどうかが決まります。エージェントアップデートにおける IPv6 サポートの詳細については、234 ページの「セキュリティエージェントアップデートでの IPv6 のサポート」を参照してください。

セキュリティエージェントの標準のアップデート元の設定

手順

1. [アップデート] > [エージェント] > [アップデート元]に移動します。
2. [標準アップデート元 (Apex One サーバからのアップデート)] を選択します。
3. [すべてのエージェントに通知] をクリックします。

セキュリティエージェントアップデートプロセス

注意

ここでは、セキュリティエージェントのアップデートプロセスについて説明します。アップデートエージェントのアップデートプロセスについては、234 ページの「セキュリティエージェントの標準のアップデート元」で説明します。

セキュリティエージェントを Apex One サーバから直接アップデートするように設定した場合、アップデートプロセスは次のように実行されます。

1. セキュリティエージェントが Apex One サーバからアップデートを取得します。
2. Apex One サーバからアップデートできない場合、次のオプションが有効であれば、セキュリティエージェントはトレンドマイクロのアップデートサーバに直接接続を試みます: [エージェント] > [エージェント管理] の [設定] > [権限とその他の設定] > [その他の設定] (タブ) > [アップデート設定] で、[セキュリティエージェントがトレンドマイクロのアップデートサーバからアップデートをダウンロード]

注意

トレンドマイクロのアップデートサーバからアップデートできるのはコンポーネントのみです。ドメイン設定、プログラム、および HotFix は、Apex One サーバまたはアップデートエージェントからのみダウンロードできます。パターンファイルのみをトレンドマイクロのアップデートサーバからダウンロードするようにセキュリティエージェントを設定すると、アップデートプロセスを高速化できます。詳細については、241 ページの「セキュリティエージェントのアップデート元としてのアップデートサーバ」を参照してください。

セキュリティエージェントのユーザ指定のアップデート元

セキュリティエージェントは、Apex One サーバの他に、ユーザ指定のアップデート元からもアップデートできます。ユーザ指定のアップデート元を使用すると、セキュリティエージェントから Apex One サーバへのアップデートトラフィックを減らすことができ、Apex One サーバに接続できないセキュリティエージェントでも適切なタイミングでのアップデートが可能になります。[ユーザアップデート元リスト] でユーザ指定のアップデート元を指定します。ここでは、1024 までのアップデート元を指定できます。

ヒント

アップデートエージェントとしていくつかのセキュリティエージェントを割り当てて、それらをこの一覧に追加することをお勧めします。

セキュリティエージェントのユーザ指定のアップデート元の設定

重要

ウイルスバスター Corp. XG Service Pack 1 (以降) では、アップデートエージェントとセキュリティエージェントの間の通信プロトコルに HTTPS を使用することができます。通信プロトコルを HTTPS に変更する前に、アップデートエージェントとそのエージェントに接続されているすべてのセキュリティエージェントをウイルスバスター Corp. XG Service Pack 1 (以降) にバージョンアップする必要があります。

手順

1. [アップデート] > [エージェント] > [アップデート元]に移動します。
2. [ユーザ指定アップデート元] を選択します。
3. アップデートエージェントとセキュリティエージェントがアップデートを受信する方法を選択します。
   - アップデートエージェントの場合は、Apex One サーバからのみアップデートを実行する (コンポーネント、ドメイン設定、エージェントプログラム、および HotFix のアップデート)
   - 利用できるユーザ指定アップデート元が見つからない場合、Apex One サーバから次のデータをアップデートする:
     - コンポーネント
     - ドメイン設定
     - セキュリティエージェントプログラムと HotFix

   詳細については、235 ページの「セキュリティエージェントアップデートプロセス」を参照してください。
4. 1 つ以上のアップデートエージェントをアップデート元として指定した場合は、[アップデート元の分析レポート] をクリックしてエンドポイントのアップデートの状態の概要を示すレポートを生成します。

   このレポートの詳細については、267 ページの「アップデート元の分析レポート」を参照してください。
5. [ユーザアップデート元リスト] に対して追加または編集を行います。
   - 新しいアップデート元を指定する場合は、[追加] をクリックします。
   - 既存のアップデート元を編集する場合は、[IP 範囲] 列の値をクリックします。

   注意

   既存のウイルスバスター Corp. XG SP1 (以降) アップデートエージェントの通信プロトコルを HTTPS に変更する場合は、既存のアップデート元を編集します。

[IP アドレスの範囲とアップデート元の追加/編集] 画面が表示されます。

6. アップデート元からアップデートを受信するエンドポイントの IP アドレスを設定します。

   - IPv4: アップデート元を使用するエンドポイントの IPv4 アドレス範囲を指定します。
   - IPv6: アップデート元を使用するエンドポイントの IPv6 のプレフィックスと長さを指定します。

   注意

   セキュリティエージェントから IP アドレスを使用してアップデート元に接続できることを確認してください。たとえば、IPv4 アドレス範囲を指定した場合、アップデート元にも IPv4 アドレスが必要です。IPv6 のプレフィックスと長さを指定した場合、アップデート元にも IPv6 アドレスが必要です。

   エンドポイントアップデートにおける IPv6 サポートの詳細については、233 ページの「セキュリティエージェントのアップデート元」を参照してください。

7. アップデート元を指定します。アップデートエージェントを選択するか (アップデートエージェントが割り当て済みの場合)、または特定のアップデート元の URL を入力します。

   - URL: アップデート元の URL を指定します。

     注意

     既存のアップデートエージェントのプロトコルを HTTP から HTTPS に変更するには、[URL] の値を変更します。

   - アップデートエージェント: 事前設定済みのアップデートエージェントをドロップダウンから選択し、セキュリティエージェントがアップデートエージェントに接続する方法を選択します。
     - アップデートエージェントの IP アドレスを使用して接続する
     - アップデートエージェントのホスト名を使用して接続する

注意

アップデートエージェントがウイルスバスター Corp. XG SP1 以降にアップデートされている場合は、HTTPS プロトコルを使用するように Apex One が自動的に外部ソース URL を設定します。

8. [保存] をクリックします。
9. [ユーザアップデート元リスト] を管理します。
   a. リストからアップデート元を削除するには、チェックボックスをオンにして [削除] をクリックします。
   b. アップデート元を移動するには、上矢印または下矢印をクリックします。一度に移動できるのは 1 つのアップデート元のみです。
10. [すべてのエージェントに通知] をクリックします。

セキュリティエージェントアップデートプロセス

注意

ここでは、セキュリティエージェントのアップデートプロセスについて説明します。アップデートエージェントのアップデートプロセスについては、263 ページの「ユーザ指定のアップデートエージェントのアップデート元」で説明します。

ユーザ指定のアップデート元のリストを設定して保存すると、アップデート処理が次のように実行されます。

1. セキュリティエージェントは、リストの 1 番目のアップデート元からのアップデートを試みます。
2. リストの 1 番目のアップデート元からアップデートできない場合には、リストの 2 番目のアップデート元からのアップデートを試み、アップデートできない場合には、以下同様の処理が続けられます。
3. すべてのアップデート元からアップデートできない場合、[アップデート元] 画面の次の設定が確認されます。

表 6-6. ユーザ指定アップデート元の追加設定

設定	説明
アップデートエージェントの場合は、Apex One サーバからのみアップデートを実行する (コンポーネント、ドメイン設定、エージェントプログラム、および HotFix のアップデート)	この設定が有効な場合、アップデートエージェントは Apex One サーバから直接アップデートし、[ユーザアップデート元リスト] は無視します。 これが無効な場合、アップデートエージェントは標準エージェント用のユーザ指定アップデート元設定を適用します。
利用できるユーザ指定アップデート元が見つからない場合、Apex One サーバから次のデータをアップデートする:	
コンポーネント	この設定が有効な場合、エージェントは Apex One サーバからコンポーネントをアップデートします。 無効な場合、次のいずれかの項目に該当するときには、エージェントはトレンドマイクロのアップデートサーバへの直接接続を試行します。 • [エージェント] > [エージェント管理]の [設定] > [権限とその他の設定] > [その他の設定] (タブ) > [アップデート設定] で、[セキュリティエージェントがトレンドマイクロのアップデートサーバからアップデートをダウンロード] オプションが有効になっている。 • トレンドマイクロのアップデートサーバが [ユーザアップデート元リスト] に含まれていない。 **注意** トレンドマイクロのアップデートサーバからアップデートできるのはコンポーネントのみです。ドメイン設定、プログラム、および HotFix は、Apex One サーバまたはアップデートエージェントからのみダウンロードできます。パターンファイルのみをトレンドマイクロのアップデートサーバからダウンロードするようにエージェントを設定すると、アップデートプロセスを高速化できます。詳細については、241 ページの「セキュリティエージェントのアップデート元としてのアップデートサーバ」を参照してください。

設定	説明
ドメイン設定	この設定が有効な場合、エージェントは Apex One サーバからドメインレベルの設定をアップデートします。
セキュリティエージェントプログラムと HotFix	この設定が有効な場合、エージェントは Apex One サーバからプログラムと HotFix をアップデートします。

4. すべての使用可能なアップデート元からアップデートできない場合、エージェントはアップデート処理を終了します。

セキュリティエージェントのアップデート元としてのアップデートサーバ

セキュリティエージェントが、トレンドマイクロのアップデートサーバから直接アップデートをダウンロードする場合は、パターンファイルのみをダウンロードするように制限して、アップデート時に消費される帯域幅を削減し、アップデートプロセスの高速化を図ることができます。

検索エンジンおよび他のコンポーネントはパターンファイルほど頻繁にアップデートされません。これがダウンロードをパターンファイルのみに限定するもう 1 つの理由です。

IPv6 シングルスタックエージェントは、トレンドマイクロのアップデートサーバから直接アップデートすることはできません。セキュリティエージェントがこれらのアップデートサーバに接続するには、DeleGate など、IP アドレスを変換できるデュアルスタックプロキシサーバが必要です。

アップデートサーバからのダウンロードの制限

手順

1. [エージェント] > [グローバルエージェント設定] に移動します。
2. [システム] タブをクリックします。
3. [アップデート] セクションに移動します。

4. [アップデートの実行時はパターンファイルのみアップデートサーバからダウンロードする] を選択します。

セキュリティエージェントのアップデート方法

Apex One サーバまたはユーザ指定のアップデート元からコンポーネントをアップデートするセキュリティエージェントでは、次のアップデート方法を使用することができます。

- 自動アップデート:エージェントのアップデートは、特定のイベントが発生したとき、または予約に基づいて自動的に実行されます。詳細については、242 ページの「セキュリティエージェントの自動アップデート」を参照してください。
- 手動アップデート:重要なアップデートがある場合には、手動アップデートを使用して、ただちにエージェントにコンポーネントのアップデートを実行するように通知します。詳細については、249 ページの「セキュリティエージェントの手動アップデート」を参照してください。
- 権限ベースのアップデート:アップデート権限のあるユーザは、コンピュータ上のセキュリティエージェントのアップデート方法をより詳細に制御できます。詳細については、251 ページの「アップデート権限とその他の設定」を参照してください。

セキュリティエージェントの自動アップデート

自動アップデートを使用すると、すべてのエージェントにアップデートを通知する負荷が軽減され、エージェントコンピュータに最新のコンポーネントがインストールされないというリスクが解消されます。

セキュリティエージェントは、自動アップデート時にコンポーネントに加えてアップデートされた設定ファイルも受け取ります。エージェントは、新しい設定を適用するために設定ファイルが必要になります。設定ファイルは、Web コンソールで Apex One 設定を変更するたびに変更されます。設定ファイルをエージェントに適用する頻度を指定する方法については、手順 3 の 245 ページの「セキュリティエージェントの自動アップデートの設定」を参照してください。

注意

自動アップデートの実行時にプロキシ設定を使用するようにエージェントを設定できます。詳細については、254 ページの「セキュリティエージェントコンポーネントのアップデートのプロキシ」を参照してください。

自動アップデートには 2 種類あります。

- 243 ページの「イベント起動配信」
- 244 ページの「予約アップデート」

イベント起動配信

サーバは、最新コンポーネントのダウンロード後に、コンポーネントをアップデートするようにオンラインのエージェントに通知することができます。また、オフラインのエージェントには、再起動してサーバに接続したときに通知することができます。必要に応じて、アップデート後にセキュリティエージェントエンドポイントで ScanNow (手動検索) を開始できます。

表 6-7. イベント起動配信のオプション

オプション	説明
Apex One サーバが新しいコンポーネントをダウンロード後、ただちにエージェントのコンポーネントのアップデートを開始する	サーバが、アップデートの完了後、ただちにエージェントにアップデートするように通知します。頻繁にアップデートされているエージェントは、差分パターンファイルをダウンロードするだけですみ、これによりアップデートにかかる時間も短縮されます (差分パターンファイルの詳細は、223 ページの「Apex One サーバコンポーネントの複製」を参照してください)。ただし、頻繁にアップデートを実行すると、サーバのパフォーマンスに悪影響を及ぼす可能性があります。特に多数のエージェントを同時にアップデートする場合には注意が必要です。 スタンドアロンモードのエージェントが存在し、それらのエージェントも同様にアップデートする場合には、[スタンドアロンモードおよびオフラインモードのエージェントを含む] を選択してください。 スタンドアロンモードの詳細については、656 ページの「セキュリティエージェントのスタンドアロンモード権限」を参照してください。

オプション	説明
再起動時、または Apex One サーバへの接続時にコンポーネントアップデートの開始を許可する (スタンドアロンモードのエージェントを除く)	アップデートを取得していないエージェントは、サーバとの接続を確立したときに、ただちにコンポーネントをダウンロードします。エージェントがオフラインの場合や、エージェントがインストールされたエンドポイントが起動されていない場合に、エージェントがアップデートを取得しないことがあります。
アップデート後、ScanNow を実行する (スタンドアロンモードのエージェントを除く)	サーバは、イベント起動配信後にエージェントに検索を実行するように通知します。特定のアップデートが、ネットワーク内にすでに拡散しているセキュリティリスクに対応するものである場合には、このオプションを有効にすることを検討してください。

注意

Apex One サーバは、コンポーネントのダウンロード後にエージェントにアップデート通知を正常に送信できない場合には、15 分後に通知を自動的に再送信します。サーバは、エージェントが応答するまで最大 5 回までアップデート通知を送信し続けます。5 回目の試行に失敗した場合、サーバは通知の送信を停止します。エージェントが再起動してサーバに接続したときにコンポーネントをアップデートするオプションを選択した場合には、引き続きコンポーネントのアップデートが実行されます。

予約アップデート

予約アップデートの実行には権限が必要です。最初に、権限を与えるセキュリティエージェントを選択する必要があります。これにより、これらのセキュリティエージェントで予約に基づいてアップデートが実行されます。

注意

予約アップデートでネットワークアドレス変換を使用する方法については、246 ページの「NAT によるセキュリティエージェントの予約アップデートの設定」を参照してください。

セキュリティエージェントの自動アップデートの設定

手順

1. [アップデート] > [エージェント] > [自動アップデート]に移動します。
2. [イベント起動配信] のイベントを選択します。
   - Apex One サーバが新しいコンポーネントをダウンロード後、ただちにエージェントのコンポーネントのアップデートを開始する
     - スタンドアロンモードおよびオフラインモードのエージェントを含む
   - 再起動時、または Apex One サーバへの接続時にコンポーネントアップデートの開始を許可する (スタンドアロンモードのエージェントを除く)
   - アップデート後、ScanNow を実行する (スタンドアロンモードのエージェントを除く)

   使用可能なオプションの詳細については、243 ページの「イベント起動配信」を参照してください。
3. [予約アップデート] のスケジュールを設定します。
   - [時間]

     [1 日 1 回のみエージェント設定の更新を行う] オプションは、毎時の頻度でアップデートのスケジュールを設定する場合に使用できます。設定ファイルには、Web コンソールを使用して指定したセキュリティエージェントの設定がすべて含まれます。

ヒント

トレンドマイクロはコンポーネントを頻繁にアップデートしますが、Apex One の設定はほとんどの場合、あまり頻繁に変更されません。コンポーネントとともに設定ファイルをアップデートすると、帯域幅の消費量が多くなり、Apex One でアップデートに必要な時間が増加します。このため、セキュリティエージェント設定は 1 日に 1 回だけアップデートすることをお勧めします。

- [毎日] または [毎週]

  アップデートの時間および Apex One サーバがエージェントにコンポーネントのアップデートを通知する期間を指定します。

  ヒント

  この設定により、指定された開始時刻にすべてのオンラインエージェントがサーバに同時に接続することを防止できるため、サーバへのトラフィック量が大幅に削減されます。たとえば、開始時刻が午後 12 時で、期間が 2 時間の場合、Apex One は午後 12 時から午後 2 時までの間、すべてのオンラインエージェントにランダムにコンポーネントをアップデートするように通知します。

注意

アップデートスケジュールの設定後、選択したエージェントでスケジュールを有効にしてください。

予約アップデートの有効化の詳細については、251 ページの「アップデート権限とその他の設定」の手順 4 を参照してください。

4. [保存] をクリックします。

   Apex One では、オフラインエージェントにただちに通知することはできません。期間終了後にオンラインになったオフラインエージェントをアップデートするには、[再起動時、または Apex One サーバへの接続時にコンポーネントアップデートの開始を許可する (スタンドアロンモードのエージェントを除く)] を選択します。この設定が有効になっていないオフラインエージェントでは、次回のスケジュール時または手動アップデート時にコンポーネントがアップデートされます。

NAT によるセキュリティエージェントの予約アップデートの設定

ローカルネットワークで NAT を使用している場合には、次の問題が発生する可能性があります。

- Web コンソールでセキュリティエージェントがオフラインと表示される
- Apex One サーバからエージェントに、アップデートと設定変更について正常に通知できない

これらの問題に対処するには、次に示すように、アップデートされたコンポーネントと設定ファイルをサーバからセキュリティエージェントに予約アップデートで配信します。

手順

- セキュリティエージェントをエージェントコンピュータにインストールする前
  a. エージェントのアップデートスケジュールを、[アップデート] > [エージェント] > [自動アップデート] の [予約アップデート] セクションで設定します。
  b. [エージェント] > [エージェント管理] で予約アップデートを有効にする権限をエージェントに与え、[設定] > [権限とその他の設定] > [権限] (タブ) > [コンポーネントのアップデート] をクリックします。
- セキュリティエージェントがエージェントコンピュータにすでに存在する場合
  a. [エージェント] > [エージェント管理] で [今すぐアップデート] を実行する権限をエージェントに与え、[設定] > [権限とその他の設定] > [権限] (タブ) > [コンポーネントのアップデート] をクリックします。
  b. ユーザに、エージェントエンドポイントでコンポーネントを手動でアップデートし (タスクトレイで [セキュリティエージェント] アイコンを右クリックして、[今すぐアップデート] をクリック)、アップデートされた設定を取得するように指示します。

セキュリティエージェントはアップデートするときに、アップデートされたコンポーネントと設定ファイルの両方を受信します。

ドメインの予約アップデートツールの使用

自動エージェントアップデートで設定されたアップデートスケジュールは、予約アップデートの権限を持つエージェントにのみ適用されます。その他のエージェントには別のアップデートスケジュールを設定できます。これを行うには、エージェントツリードメインでスケジュールを設定する必要があります。対象ドメインに属するすべてのエージェントにスケジュールが適用されます。

注意

特定のエージェントにアップデートを設定することはできません。階層ドメインの場合、子ドメインは親ドメインの設定を引き継ぎます。ただし、子ドメインの設定が別途定義されている場合は除きます。

手順

1. エージェントツリードメイン名とアップデートスケジュールを記録します。
2. <サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility¥DomainScheduledUpdate に移動します。
3. 次のファイルを<サーバインストールフォルダ>¥PCCSRV にコピーします。
   - DomainSetting.ini
   - dsu_convert.exe
4. メモ帳などのテキストエディタを使用して、DomainSetting.ini を開きます。
5. エージェントツリードメインを指定し、そのドメインのアップデートスケジュールを設定します。さらにドメインを追加するには、この手順を繰り返します。

   注意

   詳細な設定手順については、.ini ファイルを参照してください。
6. DomainSetting.ini を保存します。
7. コマンドプロンプトを開き、PCCSRV フォルダのディレクトリに移動します。
8. 次のコマンドを入力して<Enter>キーを押します。

   ```
   dsuconvert.exe DomainSetting.ini
   ```
9. Web コンソールで、[エージェント] > [グローバルエージェント設定] に移動します。

10. [保存] をクリックします。

セキュリティエージェントの手動アップデート

セキュリティエージェントのコンポーネントが著しく古いバージョンの場合、および大規模感染が発生したときには、手動でセキュリティエージェントのコンポーネントをアップデートします。セキュリティエージェントがアップデート元からコンポーネントを長期間アップデートできないと、セキュリティエージェントのコンポーネントのバージョンは古くなります。

手動アップデート時に、セキュリティエージェントはコンポーネントだけでなくアップデートされた設定ファイルも自動的に受信します。設定ファイルは新しい設定を適用するために必要です。設定ファイルは、Web コンソールで Apex One 設定を変更するたびに変更されます。

注意

手動アップデートを開始するだけではなく、手動アップデート (セキュリティエージェントエンドポイントでは [今すぐアップデート] と呼ばれます) を実行する権限をユーザに付与することもできます。詳細については、251 ページの「アップデート権限とその他の設定」を参照してください。

セキュリティエージェントの手動アップデート

手順

1. [アップデート] > [エージェント] > [手動アップデート] に移動します。
2. Apex One サーバで現在入手可能になっているコンポーネントと、これらのコンポーネントが最後にアップデートされた日付が、画面の上部に表示されます。エージェントにアップデートするように通知する前に、コンポーネントが最新であることを確認してください。

   注意

   サーバ上の旧版のコンポーネントは、手動でアップデートしてください。

   詳細については、249 ページの「セキュリティエージェントの手動アップデート」を参照してください。

3. 旧版のコンポーネントを使用しているエージェントのみをアップデートするには、次の手順を実行します。

   a. [旧版のコンポーネントを使用しているエージェントを選択] をクリックします。

   b. (オプション) 次の場合は [スタンドアロンモードおよびオフラインモードのエージェントを含む] を選択します。

      - サーバとの接続が確立されているスタンドアロンエージェントをアップデートする。
      - オフラインエージェントがオンラインになったときにアップデートする。

   c. [アップデートを開始] をクリックします。

   注意

   サーバは、このサーバのバージョンよりも古いバージョンのコンポーネントを持つエージェントを検索し、それらのエージェントにアップデートするように通知します。通知のステータスを確認するには、[アップデート] > [概要] 画面に移動します。

4. 選択したエージェントをアップデートするには、次の手順を実行します。

   a. [エージェントを手動で選択] を選択します。

   b. [選択] をクリックします。

   c. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。

   d. [アップデートを開始] をクリックします。

   注意

   サーバは各エージェントに、アップデートされたコンポーネントをダウンロードするように通知します。通知のステータスを確認するには、[アップデート] > [概要] 画面に移動します。

アップデート権限とその他の設定

アップデートの設定を行い、「今すぐアップデート」の実行や予約アップデートの有効化など、特定の権限をエージェントユーザに付与します。

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [その他の設定] タブをクリックし、[アップデート設定] セクションで次のオプションを設定します。

オプション	説明
セキュリティエージェントがトレンドマイクロのアップデートサーバからアップデートをダウンロード	アップデートの開始時、セキュリティエージェントはまず [アップデート] > [エージェント] > [アップデート元] 画面で指定されたアップデート元からアップデートを取得します。 このアップデートが失敗すると、エージェントは次に Apex One サーバからのアップデートを試行します。このオプションを選択すると、エージェントは Apex One サーバからのアップデートが失敗した場合に、トレンドマイクロのアップデートサーバからアップデートを試行できます。 **注意** IPv6 シングルスタックエージェントは、トレンドマイクロのアップデートサーバから直接アップデートすることはできません。エージェントがトレンドマイクロのアップデートサーバに接続するには、DeleGate など、IP アドレスを変換できるデュアルスタックプロキシサーバが必要です。
Apex One エージェントでの予約アップデートの有効化	このオプションを選択すると、すべてのセキュリティエージェントで、初期設定で予約アップデートが有効になるように設定されます。[予約アップデートの有効化/無効化] 権限を持つユーザはこの設定を上書きすることもできます。

オプション	説明
	アップデートスケジュールの設定方法については、245 ページの「セキュリティエージェントの自動アップデートの設定」を参照してください。
セキュリティエージェントがアップデートするコンポーネント	アップデート対象のコンポーネントを設定します。 次のオプションから選択します。 • すべてのコンポーネント (HotFix とエージェントプログラムを含む): セキュリティエージェントはすべてのコンポーネントをアップデートします。 • パターンファイル、エンジン、ドライバ: セキュリティエージェントはセキュリティエージェントプログラムのバージョンアップまたは HotFix の配信を行いません。 • パターンファイル: セキュリティエージェントはセキュリティエージェントプログラムのバージョンアップ、HotFix の配信、またはエンジンとドライバのアップデートを行いません。 注意 [すべてのコンポーネント (HotFix とエージェントプログラムを含む)] を選択すると、すべてのエージェントがサーバに同時に接続してバージョンアップまたは HotFix のインストールを実行するため、サーバのパフォーマンスが大幅に低下することがあります。

5. [権限] タブをクリックし、[コンポーネントのアップデート] セクションで次のオプションを設定します。

オプション	説明
「今すぐアップデート」の実行	この権限を持つユーザは、タスクトレイの [セキュリティエージェント] アイコンを右クリックして [今すぐアップデート] を選択することで、必要なときにコンポーネントをアップデートできます。 注意 セキュリティエージェントユーザは「今すぐアップデート」の実行時にプロキシ設定を使用できます。 詳細については、692 ページの「プロキシ設定権限の付与」を参照してください。

オプション	説明
予約アップデートの有効化/無効化	このオプションを選択すると、セキュリティエージェントユーザが、セキュリティエージェントの右クリックメニューを使用して予約アップデートを有効化および無効化できるようになります。ユーザによるこの設定は、[予約アップデートの有効化] 設定を上書きします。 注意 セキュリティエージェントのメニューにこのメニュー項目が表示されるようにするには、管理者が [その他の設定] タブで [セキュリティエージェントでの予約アップデートの有効化] を選択する必要があります。

6. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。

   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
   - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

セキュリティエージェントアップデートのディスク空き容量の設定

Apex One では、HotFix、パターンファイル、検索エンジン、およびプログラムアップデート用に一定量のエージェントのディスク容量を割り当てることができます。Apex One の初期設定では、60MB のディスク容量が確保されます。

手順

1. [エージェント] > [グローバルエージェント設定]に移動します。
2. [システム] タブをクリックします。
3. [アップデート] セクションに移動します。
4. [アップデート用に__MB のディスク容量を確保する] を選択します。
5. ディスク容量を選択します。
6. [保存]をクリックします。

セキュリティエージェントコンポーネントのアップデートのプロキシ

セキュリティエージェントは、自動アップデートの実行時や、「今すぐアップデート」を実行する権限を与えられた場合に、プロキシ設定を使用することができます。

表 6-8. セキュリティエージェントコンポーネントのアップデート時に使用するプロキシ設定

アップデート方法	使用するプロキシ設定	使用方法
自動アップデート	• 内部プロキシ設定。 詳細については、689 ページの「内部エージェントのプロキシ設定」を参照してください。	1. エージェントは、最初に内部プロキシ設定を適用します。 2. 内部プロキシ設定を行わない場合、エージェントはプロキシ設定を使用しません。

アップデート方法	使用するプロキシ設定	使用方法
今すぐアップデート	• 内部プロキシ設定。 詳細については、689 ページの「内部エージェントのプロキシ設定」を参照してください。 • ユーザが行うプロキシ設定。エージェントユーザには、プロキシ設定を行う権限を付与できます。 詳細については、692 ページの「プロキシ設定権限の付与」を参照してください。	1. エージェントは、最初に内部プロキシ設定を適用します。 2. プロキシ設定が有効ではなく、エージェントユーザが必要な権限を持っていない場合、エージェントはコンポーネントのアップデート時にプロキシを使用しません。

セキュリティエージェントのアップデート通知の設定

Apex One は、アップデート関連のイベントが発生したときに、エージェントユーザに通知します。

手順

1. [エージェント] > [グローバルエージェント設定] に移動します。
2. [エージェント制御] タブをクリックします。
3. [警告設定] セクションに移動します。
4. 次のオプションを選択します。
   - __日以上ウイルスパターンファイルがアップデートされていない場合、Windows タスクバーに警告アイコンを表示: 指定された日数より長い期間ウイルスパターンファイルがアップデートされていない場合、Windows タスクバーに警告アイコンが表示され、ユーザにウイルスパターンファイルをアップデートするように通知します。パ

ターンファイルをアップデートするには、242 ページの「セキュリティエージェントのアップデート方法」で説明されているアップデート方法のいずれかを使用します。

サーバの管理対象となるすべてのエージェントに、この設定が適用されます。

- 新しいカーネルモードドライバのロードに、エンドポイントの再起動が必要な場合は通知メッセージを表示: カーネルモードドライバの新バージョンを含む HotFix またはバージョンアップパッケージをインストールしても、前バージョンのドライバはエンドポイントから削除されません。前バージョンをアンロードして新バージョンをロードするには、エンドポイントを再起動します。エンドポイントを再起動すると、新バージョンが自動的にインストールされます。それ以降の再起動は不要です。

  エージェントエンドポイントに HotFix またはバージョンアップパッケージがインストールされた直後に、通知メッセージが表示されます。

5. [保存]をクリックします。

セキュリティエージェントアップデートログの表示

エージェントでウイルスパターンファイルをアップデートする際に問題が発生するかどうかを判断するには、エージェントアップデートログを確認します。

注意

この製品バージョンで Web コンソールからクエリできるのは、ウイルスパターンファイルのアップデートログのみです。

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログの削除スケジュールを設定します。ログの管理方法の詳細については、616 ページの「ログ管理」を参照してください。

手順

1. [ログ] > [エージェント] > [コンポーネントアップデート] に移動します。
2. エージェントのアップデート数を表示するには、[進行状況] 列内の [表示] をクリックします。表示された [コンポーネントのアップデート状況] 画面で、15 分ごとの間隔でアップデートされたエージェント数、およびアップデートされたエージェントの総数を確認します。
3. ウイルスパターンファイルをアップデートしたエージェントを表示するには、[詳細] 列の [表示] をクリックします。
4. ログを CSV ファイルに保存するには、[CSV 形式ですべてエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。

セキュリティエージェントアップデートの実行

セキュリティコンプライアンスを使用して、エージェントに最新のコンポーネントがインストールされるようにします。セキュリティコンプライアンスによって、Apex One サーバとエージェントとの間で一致しないコンポーネントが特定されます。この不一致は通常、エージェントが、コンポーネントをアップデートするためにサーバに接続できない場合に発生します。エージェントが他のアップデート元 (トレンドマイクロのアップデートサーバなど) からアップデートを取得する場合、エージェントのコンポーネントがサーバのコンポーネントより新しくなる可能性があります。

詳細については、696 ページの「管理対象エージェントのセキュリティコンプライアンス」を参照してください。

セキュリティエージェントコンポーネントのロールバック

ロールバックとは、ウイルスパターンファイル、スマートスキャンエージェントパターンファイル、およびウイルス検索エンジンを以前のバージョンに戻すことです。これらのコンポーネントが適切に機能しない場合には、前のバージョンにロールバックします。Apex One では、現在のバージョンと以前のバージョンのウイルス検索エンジン、および過去 5 バージョンのウイルスパターンファイルとスマートスキャンエージェントパターンファイルが保持されています。

注意

ロールバックできるのは上記のコンポーネントのみです。

Apex One が使用する検索エンジンは、32 ビットと 64 ビットのプラットフォームを実行するエージェントで異なります。これらの検索エンジンは個別にロールバックする必要があります。ロールバック手順はすべての種類の検索エンジンで同じです。

手順

1. [アップデート] > [ロールバック] に移動します。
2. 適切なセクションの下で、[サーバと同期] をクリックします。
   a. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
   b. [ロールバック] をクリックします。
   c. [アップデートログを表示] をクリックして、結果を確認するか、[戻る] をクリックして [ロールバック] 画面に戻ります。
3. サーバに古いバージョンのパターンファイルがある場合は、[サーバとエージェントのバージョンをロールバック] をクリックして、エージェントとサーバの両方のパターンファイルをロールバックします。

アップデートエージェント

コンポーネント、ドメイン設定、エージェントプログラム、または HotFix をセキュリティエージェントに配信するタスクを分散するために、セキュリティエージェントをアップデートエージェントに設定し、他のセキュリティエージェントのアップデート元に指定することが可能です。これにより、セキュリティエージェントは適切なタイミングでアップデートを受信でき、Apex One サーバに大量のネットワークトラフィックが集中することもありません。

ネットワークが場所によってセグメント化され、セグメント間のネットワークリンクに大量のトラフィックの負荷がかかっている場合には、それぞれの場所に少なくとも 1 つアップデートエージェントを割り当ててください。

注意

アップデートエージェントからコンポーネントをアップデートするために割り当てられたセキュリティエージェントは、アップデートエージェントから最新コンポーネントおよび設定のみを受信します。ただし、すべてのセキュリティエージェントは Apex One サーバにステータスを報告します。

アップデートエージェントのシステム要件

システム要件の完全なリストについては、次の Web サイトを参照してください。

http://www.go-tm.jp/corp/req

アップデートエージェント設定

アップデートエージェント設定は、次の 2 つのステップで実行します。

1. セキュリティエージェントを特定のコンポーネント用のアップデートエージェントとして割り当てます。
2. このアップデートエージェントからアップデートするエージェントを指定します。

注意

1 つのアップデートエージェントが処理できるエージェントの同時接続数は、エンドポイントのハードウェア仕様によって異なります。

セキュリティエージェントのアップデートエージェントとしての割り当て

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、アップデートエージェントとして指定するエージェントを選択します。

   注意

   ルートドメインアイコンは、すべてのエージェントがアップデートエージェントとして指定されることになるため選択できません。IPv6 シングルスタックのアップデートエージェントから IPv4 シングルスタックエージェントには、アップデートを直接配信することができません。同様に、IPv4 シングルスタックのアップデートエージェントから IPv6 シングルスタックエージェントにも、アップデートを直接配信することができません。このような場合に、アップデートエージェントからエージェントにアップデートを配信するには、IP アドレス変換が可能な DeleGate などのデュアルスタックプロキシサーバが必要です。

3. [設定] > [アップデートエージェント設定] の順にクリックします。
4. アップデートエージェントで共有可能な項目を選択します。
   - コンポーネントのアップデート
   - ドメイン設定
   - セキュリティエージェントプログラムと HotFix
5. [保存] をクリックします。

アップデートエージェントからアップデートするセキュリティエージェントの指定

手順

1. [アップデート] > [エージェント] > [アップデート元] に移動します。
2. [ユーザアップデート元リスト] で、[追加] をクリックします。
3. 表示された画面で、エージェントの IP アドレスを入力します。IPv4 のアドレス範囲、IPv6 のプレフィックスおよび長さ、またはその両方を入力します。
4. [アップデートエージェント] フィールドで、エージェントに割り当てるアップデートエージェントを選択します。

   注意

   エージェントから IP アドレスを使用してアップデートエージェントに接続できることを確認してください。たとえば、IPv4 アドレス範囲を指定した場合、アップデートエージェントにも IPv4 アドレスが必要です。IPv6 のプレフィックスと長さを指定した場合、アップデートエージェントにも IPv6 アドレスが必要です。
5. [保存]をクリックします。

アップデートエージェントのアップデート元

アップデートエージェントは、Apex One サーバやユーザ指定のアップデート元など、さまざまなアップデート元からアップデートを取得できます。アップデート元は、Web コンソールの [アップデート元] 画面で設定します。

アップデートエージェントの IPv6 のサポート

IPv6 シングルスタックのアップデートエージェントを、次のような IPv4 シングルスタックのアップデート元から直接アップデートすることはできません。

- IPv4 シングルスタックの Apex One サーバ
- IPv4 シングルスタックのユーザ指定のアップデート元
- トレンドマイクロのアップデートサーバ

同様に、IPv4 シングルスタックのアップデートエージェントを、IPv6 シングルスタックの Apex One サーバなど、IPv6 シングルスタックのアップデート元から直接アップデートすることはできません。

アップデートエージェントがこれらのアップデート元に接続するには、DeleGate など、IP アドレスを変換できるデュアルスタックプロキシサーバが必要です。

アップデートエージェントの標準アップデート元

Apex One サーバは、アップデートエージェントの標準のアップデート元です。アップデートエージェントを Apex One サーバから直接アップデートするように設定した場合、アップデート処理は次のように実行されます。

1. アップデートエージェントが Apex One サーバからアップデートを取得します。
2. Apex One サーバからアップデートできない場合、次のいずれかの項目に該当するときには、エージェントはトレンドマイクロのアップデートサーバへの直接接続を試行します。
   - [エージェント] > [エージェント管理]の [設定] > [権限とその他の設定] > [その他の設定] > [アップデート設定] で、[セキュリティエージェントがトレンドマイクロのアップデートサーバからアップデートをダウンロード] オプションが有効になっている。
   - トレンドマイクロのアップデートサーバが [ユーザアップデート元リスト] の最初のエントリとなっている。

ヒント

Apex One サーバからアップデートする際に問題が発生した場合にのみ、トレンドマイクロのアップデートサーバをリストの先頭に指定してください。アップデートエージェントがトレンドマイクロのアップデートサーバから直接アップデートすると、ネットワークとインターネット間で大量の帯域幅が消費されます。

3. すべての使用可能なアップデート元からアップデートできない場合、アップデートエージェントはアップデート処理を終了します。

ユーザ指定のアップデートエージェントのアップデート元

アップデートエージェントは、Apex One サーバの他に、ユーザ指定のアップデート元からもアップデートできます。ユーザ指定のアップデート元により、エージェントから Apex One サーバへのアップデートトラフィックを減らすことができます。[ユーザアップデート元リスト] でユーザ指定のアップデート元を指定します。ここでは、1024 までのアップデート元を指定できます。リストの設定手順については、236 ページの「セキュリティエージェントのユーザ指定のアップデート元」を参照してください。

注意

アップデートエージェントがユーザ指定のアップデート元に接続されるようにするには、エージェントのアップデート元画面 ([アップデート] > [エージェント] > [アップデート元]) で、[アップデートエージェントの場合は、Apex One サーバからのみアップデートを実行する (コンポーネント、ドメイン設定、エージェントプログラム、および HotFix のアップデート)] オプションを無効にしてください。

リストを設定し保存したら、次のようにアップデート処理が実行されます。

1. アップデートエージェントが、リストの 1 番目のエントリからのアップデートを試みます。
2. リストの 1 番目のエントリからアップデートできない場合には、リストの 2 番目のエントリからのアップデートを試み、アップデートできない場合には、以下同様の処理が続けられます。
3. すべてのエントリからアップデートできない場合、エージェントは、[利用できるユーザ指定アップデート元が見つからない場合、Apex One サーバから次のデータをアップデートする] で次のオプションを確認します。
   - コンポーネント:有効な場合、エージェントは Apex One サーバからアップデートされます。

     このオプションが無効な場合、次のいずれかの項目に該当するときには、エージェントはトレンドマイクロのアップデートサーバへの直接接続を試行します。

注意

コンポーネントはアップデートサーバからのみアップデートできます。ドメイン設定、プログラム、および HotFix は、サーバまたはアップデートエージェントからのみダウンロードできます。

- [エージェント] > [エージェント管理]の [設定] > [権限とその他の設定] > [その他の設定] > [アップデート設定] で、[セキュリティエージェントがトレンドマイクロのアップデートサーバからアップデートをダウンロード] オプションが有効になっている。
- トレンドマイクロのアップデートサーバが [ユーザアップデート元リスト] に含まれていない。

- ドメイン設定:有効な場合、エージェントは Apex One サーバからアップデートされます。
- セキュリティエージェントプログラムと HotFix: 有効な場合、エージェントは Apex One サーバからアップデートされます。

4. すべての使用可能なアップデート元からアップデートできない場合、アップデートエージェントはアップデート処理を終了します。

[標準アップデート元 (Apex One サーバからのアップデート)] オプションが有効で、Apex One サーバがアップデートエージェントにコンポーネントをアップデートするように通知する場合には、アップデート処理が異なったものになります。この処理は次のとおりです。

1. アップデートエージェントが直接 Apex One サーバからアップデートされ、アップデート元のリストは無視されます。
2. サーバからアップデートできない場合、次のいずれかの項目に該当するときには、エージェントはトレンドマイクロのアップデートサーバへの直接接続を試行します。
   - [エージェント] > [エージェント管理]の [設定] > [権限とその他の設定] > [その他の設定] > [アップデート設定] で、[セキュリティエージェントがトレンドマイクロのアップデートサーバからアップデートをダウンロード] オプションが有効になっている。

- トレンドマイクロのアップデートサーバが [ユーザアップデート元リスト] の最初のエントリとなっている。

ヒント

Apex One サーバからアップデートする際に問題が発生した場合にのみ、トレンドマイクロのアップデートサーバをリストの先頭に指定してください。セキュリティエージェントがトレンドマイクロのアップデートサーバから直接アップデートすると、ネットワークとインターネット間で大量の帯域幅が消費されます。

3. すべての使用可能なアップデート元からアップデートできない場合、アップデートエージェントはアップデート処理を終了します。

アップデートエージェントのアップデート元の設定

手順

1. [アップデート] > [エージェント] > [アップデート元] に移動します。
2. アップデートエージェント (Apex One サーバ) の標準アップデート元からアップデートするのか、アップデートエージェントのユーザ指定のアップデート元からアップデートするのかを選択します。
3. [すべてのエージェントに通知] をクリックします。

アップデートエージェントのコンポーネントの複製

Apex One サーバと同様に、アップデートエージェントでもコンポーネントのダウンロード時にコンポーネントの複製が使用されます。サーバがコンポーネントの複製を実行する方法の詳細については、223 ページの「Apex One サーバコンポーネントの複製」を参照してください。

アップデートエージェントのコンポーネントの複製処理は、次のようになります。

1. アップデートエージェントは、現在の完全なパターンファイルのバージョンと、アップデート元の最新バージョンを比較します。2 つのバー

ジョンの差が 14 以下の場合、アップデートエージェントは、2 つのバージョンの差分に相当する差分パターンファイルをダウンロードします。

注意

差が 14 を超える場合、アップデートエージェントは自動的にフルパターンファイルをダウンロードします。

2. アップデートエージェントで、ダウンロードした差分パターンファイルと現在の完全なパターンファイルが結合されて、最新の完全なパターンファイルが生成されます。
3. アップデートエージェントは、アップデート元の残りの差分パターンファイルをすべてダウンロードします。
4. 最新の完全なパターンファイルとすべての差分パターンファイルが、エージェントから使用可能になります。

アップデートエージェントのアップデート方法

アップデートエージェントは、通常のエージェントで使用可能なアップデート方法と同じ方法を使用します。詳細については、242 ページの「セキュリティエージェントのアップデート方法」を参照してください。

エージェントパッケージャを使用してインストールされたアップデートエージェントでは、予約アップデート設定ツールを使用して、予約アップデートを有効にし、設定することもできます。

注意

アップデートエージェントが他のインストール方法でインストールされている場合には、このツールを使用することはできません。詳細については、144 ページの「配信時の注意事項」を参照してください。

予約アップデート設定ツールの使用

手順

1. アップデートエージェントエンドポイントで、<エージェントインストールフォルダ>に移動します。
2. SUCTool.exe をダブルクリックして、ツールを実行します。予約アップデート設定ツールのコンソールが開きます。
3. [予約アップデートの有効化] を選択します。
4. アップデートの頻度と時刻を指定します。
5. [適用] をクリックします。

アップデート元の分析レポート

アップデート元の分析レポートを生成して、アップデートインフラストラクチャを分析し、アップデートエージェントやその他のアップデート元から部分的なアップデートをダウンロードするエージェントを特定します。

注意

このレポートには、アップデートエージェントから部分的なアップデートを受信するように設定されたすべてのセキュリティエージェントが含まれます。1 つまたは複数のドメインを管理するタスクを他の管理者に委任している場合、委任された管理者は、管理対象外のドメインに属しているアップデートエージェントから部分的なアップデートを受信するように設定されたすべてのセキュリティエージェントも参照できます。

アップデート元の分析レポートは、カンマ区切り形式 (.csv) のファイルにエクスポートされます。

このレポートには、次の情報が含まれています。

- セキュリティエージェント エンドポイント
- IP アドレス

- エージェントツリーのパス
- アップデート元
- エージェントが以下の項目をアップデートエージェントからダウンロードするかどうか:
  - コンポーネント
  - ドメイン設定
  - セキュリティエージェントプログラムと HotFix

重要

アップデート元の分析レポートには、アップデートエージェントから部分的なアップデートを受信するように設定されたセキュリティエージェントのみが表示されます。アップデートエージェントから完全なアップデート (コンポーネント、ドメイン設定、セキュリティエージェントプログラムと HotFix を含む) を実行するように設定されたセキュリティエージェントは表示されません。

レポート生成の詳細については、236 ページの「セキュリティエージェントのユーザ指定のアップデート元」を参照してください。

コンポーネントアップデートの概要

Web コンソールには、コンポーネントアップデートの全般的なステータスを表示する [アップデートの概要] 画面 ([アップデート] > [概要] に移動) があります。この画面で旧版のコンポーネントをアップデートできます。サーバの予約アップデートを有効にしている場合は、この画面に次のアップデートスケジュールも表示されます。

画面を定期的に更新して、最新のコンポーネントアップデートステータスを表示します。

注意

統合 Smart Protection Server でコンポーネントのアップデートを表示するには、[管理] > [Smart Protection] > [統合サーバ] に移動します。

セキュリティエージェントのアップデート状況

エージェントへのコンポーネントアップデートを開始した場合、このセクションで次の情報を参照します。

- アップデートコンポーネントを通知するエージェントの数。
- まだ通知されていないが、すでに通知キューに入っているエージェントの数。これらのエージェントに対する通知をキャンセルする場合は、[通知のキャンセル] をクリックしてください。

コンポーネント

[アップデート状況] 表で、Apex One サーバがダウンロードおよび配信した、各コンポーネントのアップデート状況を参照します。

コンポーネントごとに、現在のバージョンと最新アップデート日付が表示されます。古いバージョンのコンポーネントを持つエージェントを表示するには、数字のリンクをクリックします。古いバージョンのコンポーネントを持つエージェントを手動でアップデートします。

第 7 章

セキュリティリスクの検索

この章では、ファイルベースの検索を使用してエンドポイントをセキュリティリスクから保護する方法について説明します。

この章は次のトピックで構成されます。

セキュリティリスクについて

セキュリティリスクとは、ウイルス/不正プログラムおよびスパイウェア/グレーウェアの総称です。Apex One は、ファイルを検索して、検出されたセキュリティリスクごとに特定の処理を実行することでセキュリティリスクからエンドポイントを保護します。短期間に大量の数のセキュリティ上の脅威が検出された場合は大規模感染の兆候を示しています。Apex One は、大規模感染予防ポリシーを実行して、感染したエンドポイントが完全に危険な状態でなくなるまで隔離することで大規模感染を抑制できます。通知やログは、セキュリティリスクを監視するために利用でき、さらに即座に処理が必要な場合の警告となります。

ウイルスと不正プログラム

いまや無数のウイルス/不正プログラムが存在し、毎日作成されています。以前は DOS や Windows の世界で一般的であったエンドポイントウイルスが、今日では企業のネットワークやメールシステム、Web サイトの脆弱性などに対し、非常に大きなダメージを与えています。

表 7-1. ウイルスや不正プログラム

ウイルスや不正プログラム	説明
ジョークプログラム	ジョークプログラムは、エンドポイントの画面上にいたずらな表現を表示したりするウイルスのようなプログラムです。
その他	「その他」は、他のいずれのウイルス/不正プログラムの種類にも分類されないウイルス/不正プログラムです。
パッカー	パッカーは、圧縮され、暗号化された Windows、Linux™の実行可能プログラムで、トロイの木馬などがこれに該当します。実行ファイルを圧縮すると、ウイルス検索製品が検出するのは難しくなります。
ランサムウェア	ランサムウェアは脅威の一種であり、ファイルを暗号化、変更、またはロックして使用不能にしたのち、元に戻すことと引き換えに何らかの「身代金」を支払うよう要求するものです。一部のランサムウェアは、身代金」が期日までに支払われないとデータを自動的に削除します。

ウイルスや不正プログラム	説明
ルートキット	ルートキットは、ユーザが同意も認識もしないうちにシステムにインストールされ実行される、1 つのプログラムまたはプログラムの集合です。わかりにくい巧妙な方法で、検出されることなくコンピュータ上に存在し続けます。ルートキットは、コンピュータに感染するものではなく、実行する不正コードに対して検出されないような環境を提供しようとするものです。ルートキットは、ソーシャルエンジニアリングを用いた手口、不正プログラムの実行や不正 Web サイトの閲覧などによりコンピュータにインストールされます。インストールされると、攻撃者は、プロセス、ファイル、レジストリキーおよび通信チャネルを隠すことができるだけでなく、リモートアクセスや盗聴を含め、システム上で実質的にどのような機能でも実行できます。
テストウイルス	テストウイルスは不活性のファイルで本物のウイルスのように動作し、ウイルス検索ソフトにより検出されます。EICAR テストスクリプトのようにウイルス検索ソフトが適切に検索するかどうかテストするのに使います。
トロイの木馬	トロイの木馬プログラムは、多くの場合ポートを使用してコンピュータに侵入し、プログラムを実行します。トロイの木馬プログラムは複製は行いませんが、システムに常駐し、ポートを開いてハッカーを侵入させたりするなどの不正な処理を行います。これまでのウイルス対策ソリューションは、ウイルスを検出し、削除することはできますが、トロイの木馬 (特にすでにシステムで作動しているもの) については検出および削除できません。

ウイルスや不正プログラム	説明
ウイルス	複製を行うプログラムです。複製するために、ウイルスは自分自身を他のプログラムファイルに添付して、次のようなホストプログラムが動作するときはいつも作動します。 • ActiveX 不正コード: Web ページに内在し、ActiveX™コントロールを実行するコードです。 • システム領域感染型ウイルス: パーティションやディスクの起動セクタに感染するウイルスです。 • COM ファイルおよび EXE ファイルのウイルス: .com や.exe などの拡張子を持った実行ファイルプログラムです。 • Java 不正コード: OS 独自のウイルスで、Java™で書かれ、埋め込まれています。 • マクロウイルス: アプリケーションマクロとして暗号化され、ドキュメントに含まれているウイルスです。 • VBScript、JavaScript または HTML ウイルス: Web ページに内在し、ブラウザを通じてダウンロードされるウイルスです。 • ワーム: ワームは、ワーム自体またはその一部の動作可能なコピーを多くの場合電子メールを介して他のエンドポイントシステムに拡散できる自己完結型プログラムまたはプログラムのセットです。
ネットワークウイルス	厳密に言うと、ネットワーク上で広がるウイルスがすべてネットワークウイルスであるというわけではありません。ウイルス/不正プログラムのうちでも、ワームのように、ほんのわずかしかネットワークウイルスに該当しません。特にネットワークウイルスは、TCP、FTP、UDP、HTTP、メールプロトコルのようなネットワークプロトコルを使い、複製します。それらはシステムファイルを変えたり、ハードディスクの起動セクタを変更したりすることはめったにありません。その代わり、ネットワークウイルスはエージェントエンドポイントのメモリに感染し、トラフィックの増加をもたらし、ネットワークを遅くしさらにはネットワークダウンを引き起こします。ネットワークウイルスはメモリにとどまるので、通常のファイル I/O ベースの検索方法では検出できません。

ウイルスや不正プログラム	説明
潜在的なウイルス/不正プログラム	ウイルス/不正プログラムの特性がある不審ファイルです。 詳細については、次のトレンドマイクロの脅威データベースを参照してください。 https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/#malware 注意 潜在的なウイルス/不正プログラムに対して駆除を実行することはできませんが、検索処理は設定できます。

スパイウェアとグレーウェア

エンドポイントは、ウイルス/不正プログラム以外の潜在的な脅威からの危険性にもさらされています。スパイウェア/グレーウェアはウイルスやトロイの木馬とは異なりますが、不正な処理を実行する可能性のあるソフトウェアです。ネットワーク上のエンドポイントのパフォーマンスに悪影響を与えたり、セキュリティ、機密性、および法律に関する重大なリスクを企業に与える可能性があります。多くの場合、スパイウェア/グレーウェアは、煩わしいポップアップウィンドウの表示、ユーザのキー入力の記録、エンドポイントの脆弱性を露呈させ攻撃を受けやすくするなど、さまざまな好ましくない脅威につながる動作を実行します。

種類	説明
スパイウェア	アカウントユーザ名やパスワードなどのデータを収集し、第三者に送信します。
アドウェア	広告を表示して、ユーザの Web サーフィンの嗜好などのデータを収集します。このデータは、Web ブラウザによるそのユーザへの広告内容の設定に使用されることがあります。
ダイヤラ	エンドポイントのインターネット設定を変更し、あらかじめ設定された電話番号にエンドポイントからモデム経由でダイヤルするよう強制します。この番号は、多くの場合、ペイパーコール (pay-per-call) や国際電話の番号となっており、企業に多大な費用を負わせる可能性があります。

種類	説明
ジョークプログラム	CD-ROM トレイの開閉、多数のメッセージボックスを表示するなどエンドポイントに異常な挙動をさせます。
ハッキングツール	ハッカーがエンドポイントに入るのを助けます。
リモートアクセスツール	ハッカーがリモートアクセスしてエンドポイントをコントロールするのを助けます。
パスワード解読アプリケーション	ハッカーがアカウントユーザ名やパスワードを解読するのを助けます。
その他	上記のどの種類にも該当しないスパイウェア/グレーウェアです。

スパイウェア/グレーウェアがネットワークに侵入する方法

スパイウェア/グレーウェアが企業ネットワークに侵入する経路としては、インストールパッケージにグレーウェアアプリケーションが含まれている正規ソフトウェアをユーザがダウンロードするケースがあります。ほとんどのソフトウェアプログラムにはエンドユーザ使用許諾契約書が含まれており、ユーザはダウンロードする前にその内容に同意する必要があります。実際のところ、エンドユーザ使用許諾契約書にはアプリケーションおよびその使用目的として個人データの収集が記載されていることは珍しくありません。ただし、ユーザがこの情報を見落とす場合や、法律用語を正しく理解しない場合があります。

潜在的リスクと脅威

ネットワーク上にスパイウェアやその他の種類のグレーウェアが存在すると、次のような状況になる可能性があります。

表 7-2. 潜在的リスクと脅威

リスクまたは脅威	説明
エンドポイントのパフォーマンス低下	これらのタスクを実行するために、スパイウェア/グレーウェアはしばしばかなりの CPU とシステムメモリリソースを必要とします。
Web ブラウザのクラッシュの増加	ある種のグレーウェアは、アドウェアのようにブラウザフレームや Windows に情報を何度も表示します。これらのアプリケーションのコードがシステムプロセスとどのような相互作用をするかによって、グレーウェアは時々ブラウザをクラッシュさせたり、フリーズさせたり、さらにはエンドポイントの再起動を要求することもあります。
ユーザ効率の低下	頻繁に生じるポップアップ広告やジョークプログラムのマイナス効果に悩まされ、ユーザはその主たる業務が必要以上に散漫になってしまいます。
ネットワーク速度の低下	スパイウェア/グレーウェアは集めた情報をネットワーク上で動作する他のアプリケーションや、外部に定期的に伝えたりします。
個人情報、企業情報の損失	スパイウェア/グレーウェアが集めるデータは、ユーザが訪問する Web サイトのリストのような情報だけではありません。スパイウェア/グレーウェアは、オンライン銀行口座や企業ネットワークにアクセスするためなどに使用するユーザアカウント情報を集める場合もあります。
法的責任のリスク増加	ネットワーク上のエンドポイントリソースがハイジャックされると、ハッカーは企業のエージェントコンピュータを利用して攻撃をしかけたり、ネットワーク外のコンピュータにスパイウェア/グレーウェアをインストールすることもあります。このような活動でネットワークリソースに関与した場合、他の団体が受ける損害に対して、企業に法的な責任が発生する可能性があります。

スパイウェア/グレーウェアとその他の脅威に対する防御

エンドポイントにスパイウェア/グレーウェアをインストールすることを防御する方法はいくつかあります。トレンドマイクロは、次のような方法をお勧めします。

- すべての種類の検索 (手動検索、リアルタイム検索、予約検索、および ScanNow) を設定して、スパイウェア/グレーウェアのファイルとアプリ

ケーションを検索および削除できるようにします。詳細については、285 ページの「検索の種類」を参照してください。

- エージェントユーザに、次のようなことを指導します。
  - エージェントユーザがダウンロードして自分たちのコンピュータにインストールするアプリケーションのエンドユーザ使用許諾契約書 (EULA) と付属ドキュメントを読むこと。
  - ソフトウェアをダウンロードしてインストールする許可を求めるメッセージに対しては、エージェントユーザがソフトウェアの作成者と閲覧している Web サイトを信頼できると確信できない場合は、[いいえ] をクリックすること。
  - 未承諾広告メール (スパムメール)、特にスパムメールがユーザにボタンやハイパーリンクをクリックするよう求めている場合は無視すること。
- Web ブラウザを厳しいセキュリティレベルに設定してください。トレンドマイクロは、ActiveX コントロールをインストールする前に Web ブラウザがユーザに確認を求めるようにすることをお勧めします。
- Microsoft Outlook を使っている場合は、スパムメールで送られる画像ファイルのように Microsoft Outlook が HTML アイテムを自動的にダウンロードしないようなセキュリティ設定にしてください。
- ピアツーピアのファイル共有サービスを使用できないようにしてください。スパイウェアや他のグレーウェアアプリケーションは、MP3 ミュージックファイルなどのように、ユーザがダウンロードしたくなるような別の種類のファイルにマスクされている場合があります。
- エージェントコンピュータにインストールしたソフトウェアを定期的に調べて、スパイウェアや他のグレーウェアの可能性があるアプリケーションを探してください。
- Windows の OS に Microsoft からの最新パッチを適用してください。詳細は Microsoft の Web サイトを参照してください。

検索方法の種類

セキュリティエージェントでは、セキュリティリスクの検索時に 2 つの検索方法のどちらかを使用できます。1 つはスマートスキャンで、もう 1 つは従来型スキャンです。

- スマートスキャン

  このヘルプでは、スマートスキャンを使用するセキュリティエージェントを「スマートスキャンエージェント」と呼びます。スマートスキャンエージェントは、ローカル検索と、ファイルレピュテーションサービスで提供されるクラウド型クエリを利用できます。

- 従来型スキャン

  スマートスキャンを使用しないエージェントは、「従来型スキャンエージェント」と呼ばれます。従来型スキャンエージェントでは、エンドポイント上にすべてのセキュリティエージェントコンポーネントが格納され、ローカルのすべてのファイルが検索されます。

初期設定の検索方法

本バージョンの Apex One の新規インストールにおける、初期設定の検索方法はスマートスキャンです。つまり、Apex One サーバの新規インストールを実行した後に、Web コンソールで検索方法を変更しなければ、そのサーバによって管理されるすべてのエージェントはスマートスキャンを使用します。

Apex One サーバを以前のバージョンからバージョンアップし、エージェントの自動バージョンアップを有効にしている場合、そのサーバによって管理されるすべてのエージェントはバージョンアップ前に設定された検索方法を継続して使用します。たとえば、スマートスキャンと従来型スキャンをサポートする以前のバージョンの Apex One からのバージョンアップでは、スマートスキャンを使用するエージェントはすべてスマートスキャンを、従来型スキャンを使用するエージェントはすべて従来型スキャンを継続して使用します。

検索方法の比較

次の表は、2 つの検索方法を比較したものです。

表 7-3. 従来型スキャンとスマートスキャンの比較

比較基準	従来型スキャン	スマートスキャン
検索動作	従来型スキャンセキュリティエージェントが、ローカルエンドポイントで検索を実行します。	• スマートスキャンセキュリティエージェントが、ローカルエンドポイントで検索を実行します。 • セキュリティエージェントが検索時にファイルの危険性を判定できない場合には、セキュリティエージェントが検索クエリを Trend Micro Smart Protection ソースに送信して危険性を検証します。 • 検索のパフォーマンスを向上させるために、セキュリティエージェントでは検索クエリの結果を「キャッシュ」できます。
使用中および更新されたコンポーネント	アップデート元で利用可能なすべてのコンポーネント (スマートスキャンエージェントパターンファイルを除く)	アップデート元で利用可能なすべてのコンポーネント (ウイルスパターンファイルおよびスパイウェア監視パターンファイルを除く)
通常のアップデート元	Apex One サーバ	Apex One サーバ

検索方法の変更

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [検索設定] > [検索方法] の順にクリックします。

4. [従来型スキャン] または [スマートスキャン] を選択します。
5. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。
   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
   - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

スマートスキャンから従来型スキャンへの切り替え

次の表は、セキュリティエージェントで使用する検索方法を切り替える前の注意事項を示しています。

1. 切り替えるセキュリティエージェントの数

   一度に切り替えるセキュリティエージェントの数を比較的少数にすることで、Apex One サーバおよび Smart Protection Server のリソースを効率的に使用することができます。これらのサーバは、セキュリティエージェントが検索方法を変更しても、他の重要なタスクを実行できます。

2. タイミング

   検索方法を切り替える場合、セキュリティエージェントでは、新しい検索方法に必要なフルパターンファイルをダウンロードする必要があります。

   ネットワーク帯域幅への影響とユーザの日常業務の中断を避けるために、就業時間帯を避けて切り替えることを検討してください。検索方法を切り替える際、セキュリティエージェントで [今すぐアップデート] が使用できないように設定をしておくことをお勧めします。

3. エージェントツリー設定

検索方法は、ルート、ドメイン、または個別のセキュリティエージェントレベルで適用できる、細かい設定です。検索方法を切り替えると、次の操作を行うことができます。

- 新しいエージェントツリードメインを作成し、その検索方法として従来型スキャンを割り当てます。このドメインに移動したすべてのエージェントは、従来型スキャンを使用します。エージェントを移動するときは、[選択したエージェントに新しいドメインの設定を適用する] の設定を有効にします。
- ドメインを選択し、従来型スキャンを使用するように設定します。そのドメインに属するスマートスキャンエージェントは、従来型スキャンに切り替わります。
- ドメインから 1 つ以上のスマートスキャンエージェントを選択し、従来型スキャンに切り替えます。

注意

ドメインの検索方法に対する変更は、個々のエージェントに設定した検索方法よりも優先されます。

従来型スキャンからスマートスキャンへの切り替え

従来型スキャンからスマートスキャンにエージェントを切り替える場合には、Trend Micro Smart Protection サービスが設定されていることを確認してください。

詳細については、113 ページの「Trend Micro Smart Protection サービスの設定」を参照してください。

次の表は、スマートスキャンに切り替えるときのその他の注意点を示しています。

表 7-4. スマートスキャンへ切り替える際の注意事項

注意事項	詳細
製品ライセンス	スマートスキャンを使用するには、ライセンスが次のサービスに対してアクティベート済みで、さらにサポート契約期限切れでないことを確認します。 • ウイルス対策 • Web レピュテーションおよびスパイウェア対策
Apex One サーバ	エージェントが Apex One サーバに接続可能であることを確認します。スマートスキャンに切り替わったことが通知されるのは、オンラインエージェントのみです。オフラインエージェントは、オンラインになったときに通知されます。スタンドアロンモードのエージェントは、オンラインになったときに通知されるか、またはエージェントに予約アップデートの権限がある場合には、予約アップデートの実行時に通知されます。 また、Apex One サーバに最新のコンポーネントがインストールされていることも確認してください。これは、スマートスキャンエージェントが、サーバからスマートスキャンエージェントパターンファイルをダウンロードする必要があるためです。 コンポーネントをアップデートする方法については、218 ページの「Apex One サーバのアップデート」を参照してください。
切り替えるエージェントの数	一度に切り替えるエージェントの数を比較的少数にすることで、Apex One サーバのリソースを効率的に使用することができます。Apex One サーバは、エージェントが検索方法を変更しても、他の重要なタスクを実行できます。
タイミング	エージェントは、初めてスマートスキャンに切り替えるときに、Apex One サーバからスマートスキャンエージェントのフルパターンファイルをダウンロードする必要があります。スマートスキャンパターンファイルは、スマートスキャンエージェントでのみ使用されます。 ダウンロードプロセスを短時間で終了させるために、就業時間帯を避けて切り替えることを検討してください。また、サーバからエージェントをアップデートする予定がないときに切り替えることを検討してください。さらに、エージェントでの「今すぐアップデート」を一時的に無効にして、エージェントがスマートスキャンに切り替わってから再度有効にしてください。

注意事項	詳細
エージェントツリー設定	検索方法は、ルート、ドメイン、または個別のエージェントレベルで設定できる、細かい設定です。スマートスキャンに切り替えると次の操作が可能になります。 • 新しいエージェントツリードメインを作成し、その検索方法としてスマートスキャンを割り当てます。このドメインに移動したすべてのエージェントは、スマートスキャンを使用します。エージェントを移動するときは、[選択したエージェントに新しいドメインの設定を適用する] の設定を有効にします。 • ドメインを選択し、スマートスキャンを使用するように設定します。そのドメインに属する従来型スキャンエージェントは、スマートスキャンに切り替わります。 • ドメインから 1 つ以上の従来型スキャンエージェントを選択し、スマートスキャンに切り替えます。 **注意** ドメインの検索方法に対する変更は、個々のエージェントに設定した検索方法よりも優先されます。
IPv6 のサポート	スマートスキャンエージェントは、検索クエリを Trend Micro Smart Protection ソースに送信します。 IPv6 シングルスタックのスマートスキャンエージェントからは、次のような IPv4 シングルスタックソースに直接クエリを送信することはできません。 • Protection Network 同様に、IPv4 シングルスタックのスマートスキャンエージェントからは、IPv6 シングルスタックの Smart Protection Server にクエリを送信することはできません。 スマートスキャンエージェントがこれらのソースに接続するには、DeleGate など、IP アドレスを変換できるデュアルスタックプロキシサーバが必要です。

検索の種類

Apex One では、セキュリティエージェントコンピュータをセキュリティリスクから保護するために、次の検索の種類を提供しています。

表 7-5. 検索の種類

検索の種類	説明
リアルタイム検索	エンドポイント内のファイルが、受信時、開いたとき、ダウンロード時、コピー時、および変更時に自動的に検索されます。 詳細については、285 ページの「リアルタイム検索」を参照してください。
手動検索	ユーザが要求したファイル (またはファイルのセット) を検索する手動の検索です。 詳細については、288 ページの「手動検索」を参照してください。
予約検索	管理者やエージェントユーザが設定したスケジュールに従って、エンドポイント内のファイルが自動的に検索されます。 詳細については、291 ページの「予約検索」を参照してください。
ScanNow	1 つ以上の対象コンピュータ内にあるファイルを検索する、管理者が開始する検索です。 詳細については、293 ページの「ScanNow」を参照してください。

リアルタイム検索

リアルタイム検索は、継続的に実行される検索です。ファイルの受信時、開かれたとき、ダウンロード時、コピー時、または変更時に毎回、ファイルにセキュリティリスクが存在するかどうかを調べるリアルタイム検索が実行されます。セキュリティエージェントでセキュリティリスクが検出されなかった場合、ユーザはそのファイルへのアクセスを続けることができます。セキュリティエージェントがセキュリティリスクまたは潜在的なウイルス/不正プログラムを検出した場合、通知メッセージが表示され、感染ファイルの名前と該当するセキュリティリスクが示されます。

リアルタイム検索は検索キャッシュを保持し、セキュリティエージェントが起動するたびにキャッシュが再ロードされます。セキュリティエージェント

は、セキュリティエージェントのアンロード後に行われたファイルまたはフォルダへの変更を追跡し、変更があったファイルをキャッシュから削除します。

注意

通知メッセージを変更するには、Web コンソールを開いて、[管理] > [通知] > [エージェント] に移動します。

リアルタイム検索設定を、1 つ以上のセキュリティエージェントおよびドメインに設定および適用するか、またはサーバが管理するすべてのセキュリティエージェントに設定および適用します。

リアルタイム検索設定

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [検索設定] > [リアルタイム検索設定] の順にクリックします。
4. 次のオプションを選択します。
   - ウイルス/不正プログラム検索を有効にする
   - スパイウェア/グレーウェア検索を有効にする

   注意

   ウイルス/不正プログラムの検索を無効にすると、スパイウェア/グレーウェアの検索も無効になります。ウイルスの大規模感染の間は、ウイルスによってエージェントコンピュータ上のファイルやフォルダが変更または削除されるのを防ぐために、リアルタイム検索を無効にすることはできません (初期状態で無効の場合には、自動的に有効になります)。

5. [対象] タブで、次の設定を行います。
   - 297 ページの「ファイルに対するユーザのアクティビティ」
   - 298 ページの「検索対象ファイル」
   - 298 ページの「検索設定」
6. [処理] タブをクリックして、次の設定を行います。

表 7-6. 検出時の処理

処理	レファレンス/参照情報
ウイルス/不正プログラムの処理	1 次処理 (1 つを選択): • 310 ページの「トレンドマイクロの推奨処理を使用」 • 311 ページの「すべての種類のウイルス/不正プログラムに同じ処理を使用」 • 312 ページの「特定の処理を検出されたウイルス/不正プログラムの種類ごとに使用」 注意 各処理の詳細については、308 ページの「ウイルス/不正プログラムの検出時の処理」を参照してください。 追加のウイルス/不正プログラムの処理: • 312 ページの「隔離ディレクトリ」 • 314 ページの「ウイルス駆除実行前にバックアップを作成」 • 314 ページの「ダメージクリーンナップサービス」 • 316 ページの「ウイルス/不正プログラムの検出時に通知を表示する」 • 316 ページの「潜在的なウイルス/不正プログラムの検出時に通知を表示する」

処理	レファレンス/参照情報
スパイウェア/グレーウェアの処理	1 次処理: • 321 ページの「スパイウェア/グレーウェアの検出時の処理」 追加のスパイウェア/グレーウェアの処理: • 323 ページの「スパイウェア/グレーウェアの検出時に通知を表示する」

7. [検索除外] タブで、検索から除外するディレクトリ、ファイル、および拡張子を設定します。

   詳細については、302 ページの「検索除外」を参照してください。

8. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。

   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
   - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

手動検索

手動検索はオンデマンドの検索であり、ユーザがセキュリティエージェントコンソールで検索を実行するとただちに開始されます。検索にかかる時間は、検索するファイル数やセキュリティエージェントエンドポイントのハードウェアリソースによって異なります。

手動検索設定を、1 つ以上のエージェントおよびドメインに設定および適用するか、またはサーバが管理するすべてのエージェントに設定および適用します。

手動検索設定

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [検索設定] > [手動検索設定] の順にクリックします。
4. [対象] タブで、次の設定を行います。
   - 298 ページの「検索対象ファイル」
   - 298 ページの「検索設定」
   - 301 ページの「CPU 使用率」
5. [処理] タブをクリックして、次の設定を行います。

表 7-7. 検出時の処理

処理	レファレンス/参照情報
ウイルス/不正プログラムの処理	1 次処理 (1 つを選択): • 310 ページの「トレンドマイクロの推奨処理を使用」 • 311 ページの「すべての種類のウイルス/不正プログラムに同じ処理を使用」 • 312 ページの「特定の処理を検出されたウイルス/不正プログラムの種類ごとに使用」 注意 各処理の詳細については、308 ページの「ウイルス/不正プログラムの検出時の処理」を参照してください。 追加のウイルス/不正プログラムの処理: • 312 ページの「隔離ディレクトリ」 • 314 ページの「ウイルス駆除実行前にバックアップを作成」 • 314 ページの「ダメージクリーンナップサービス」
スパイウェア/グレーウェアの処理	1 次処理: • 321 ページの「スパイウェア/グレーウェアの検出時の処理」

6. [検索除外] タブで、検索から除外するディレクトリ、ファイル、および拡張子を設定します。

   詳細については、302 ページの「検索除外」を参照してください。

7. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。

   • すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェン

トに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。

- 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

予約検索

予約検索は指定された日時に自動的に実行されます。エージェントの予約検索により検索ルーチンを自動化すれば、検索の管理効率を改善できます。

予約検索設定を、1 つ以上のエージェントおよびドメインに設定および適用するか、またはサーバが管理するすべてのエージェントに設定および適用します。

予約検索設定

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [検索設定] > [予約検索設定] の順にクリックします。
4. 次のオプションを選択します。
   - ウイルス/不正プログラム検索を有効にする
   - スパイウェア/グレーウェア検索を有効にする

注意

スパイウェア検索を有効にするには、ウイルス/不正プログラムの検索を有効にする必要があります。

5. [対象] タブで、次の設定を行います。
   - 301 ページの「スケジュール」
   - 298 ページの「検索対象ファイル」
   - 298 ページの「検索設定」
   - 301 ページの「CPU 使用率」
6. [処理] タブをクリックして、次の設定を行います。

表 7-8. 検出時の処理

処理	レファレンス/参照情報
ウイルス/不正プログラムの処理	1 次処理 (1 つを選択): • 310 ページの「トレンドマイクロの推奨処理を使用」 • 311 ページの「すべての種類のウイルス/不正プログラムに同じ処理を使用」 • 312 ページの「特定の処理を検出されたウイルス/不正プログラムの種類ごとに使用」 注意 各処理の詳細については、308 ページの「ウイルス/不正プログラムの検出時の処理」を参照してください。 追加のウイルス/不正プログラムの処理: • 312 ページの「隔離ディレクトリ」 • 314 ページの「ウイルス駆除実行前にバックアップを作成」 • 314 ページの「ダメージクリーンナップサービス」 • 316 ページの「ウイルス/不正プログラムの検出時に通知を表示する」 • 316 ページの「潜在的なウイルス/不正プログラムの検出時に通知を表示する」

処理	レファレンス/参照情報
スパイウェア/グレーウェアの処理	1 次処理: • 321 ページの「スパイウェア/グレーウェアの検出時の処理」 追加のスパイウェア/グレーウェアの処理: • 323 ページの「スパイウェア/グレーウェアの検出時に通知を表示する」

7. [検索除外] タブで、検索から除外するディレクトリ、ファイル、および拡張子を設定します。

   詳細については、302 ページの「検索除外」を参照してください。

8. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。

   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
   - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

ScanNow

ScanNow は、管理者によって Web コンソールを通してリモートで開始され、1 つ以上のセキュリティエージェントエンドポイントを対象にすることができます。

ScanNow 設定を、1 つ以上のセキュリティエージェントおよびドメインに設定および適用するか、またはサーバが管理するすべてのセキュリティエージェントに設定および適用します。

ScanNow 設定

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [検索設定] > [ScanNow 設定] の順にクリックします。
4. 次のオプションを選択します。
   - ウイルス/不正プログラム検索を有効にする
   - スパイウェア/グレーウェア検索を有効にする

   注意

   スパイウェア検索を有効にするには、ウイルス/不正プログラムの検索を有効にする必要があります。
5. [対象] タブで、次の設定を行います。
   - 298 ページの「検索対象ファイル」
   - 298 ページの「検索設定」
   - 301 ページの「CPU 使用率」
6. [処理] タブをクリックして、次の設定を行います。

表 7-9. 検出時の処理

処理	レファレンス/参照情報
ウイルス/不正プログラムの処理	1 次処理 (1 つを選択): • 310 ページの「トレンドマイクロの推奨処理を使用」 • 311 ページの「すべての種類のウイルス/不正プログラムに同じ処理を使用」 • 312 ページの「特定の処理を検出されたウイルス/不正プログラムの種類ごとに使用」 注意 各処理の詳細については、308 ページの「ウイルス/不正プログラムの検出時の処理」を参照してください。 追加のウイルス/不正プログラムの処理: • 312 ページの「隔離ディレクトリ」 • 314 ページの「ウイルス駆除実行前にバックアップを作成」 • 314 ページの「ダメージクリーンナップサービス」
スパイウェア/グレーウェアの処理	1 次処理: • 321 ページの「スパイウェア/グレーウェアの検出時の処理」

7. [検索除外] タブで、検索から除外するディレクトリ、ファイル、および拡張子を設定します。

   詳細については、302 ページの「検索除外」を参照してください。

8. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。

   • すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェン

トに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。

- 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

ScanNow の開始

感染の疑いがあるコンピュータで ScanNow を開始します。

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [タスク] > [ScanNow] をクリックします。
4. 検索を開始する前に、事前設定された ScanNow 設定を変更するには、[設定] をクリックします。

   [ScanNow 設定] 画面が開きます。詳細については、293 ページの「ScanNow」を参照してください。
5. エージェントツリーで、検索を実行するエージェントを選択し、[ScanNow を開始] をクリックします。

   サーバがエージェントに通知します。
6. 通知のステータスをチェックし、通知を受信していないエージェントがないか確認します。
7. [未通知のエンドポイントを選択] > [ScanNow を開始] の順にクリックすると、未通知のエージェントにただちに通知が再送信されます。

   例:エージェント総数: 50

表 7-10. 未通知のエージェントのシナリオ

エージェントツリーでの選択	通知済みのエージェント ([ScanNow を開始] のクリック後)	未通知のエージェント
なし (50 のエージェントすべてを自動的に選択)	50 のエージェントのうち 35 のエージェント	15 エージェント
手動選択 (50 のエージェントのうち 45 のエージェントを選択)	45 のエージェントのうち 40 のエージェント	5 つのエージェント、および手動選択に含まれない別の 5 つのエージェント

8. [通知の中止] をクリックして、現在通知中のエージェントへの通知を停止するように Apex One に指示します。このコマンドは、通知済みのエージェントおよび検索処理中のエージェントでは無視されます。
9. 検索処理をすでに実行中のエージェントについては、[ScanNow を中止] をクリックして検索の停止を通知します。

すべての検索の種類に共通の設定

検索の種類ごとに、検索条件、検索除外、および検出時の処理の 3 つを設定します。これらの設定を 1 つ以上のエージェントおよびドメインに配信するか、またはサーバが管理するすべてのエージェントに配信します。

検索条件

ファイルの種類や拡張子などのファイル属性を使用して、特定の検索の種類で検索するファイルを指定します。また、検索を実行する条件を指定します。たとえば、ファイルがエンドポイントにダウンロードされるたびに検索するよう、リアルタイム検索を設定します。

ファイルに対するユーザのアクティビティ

リアルタイム検索を実行するファイルに対するアクティビティを指定します。次のオプションから選択します。

- 作成された/変更されたファイル:エンドポイントに (ファイルのダウンロード後などに) 取り込まれた新しいファイル、または変更されたファイルを検索します。
- 読み込まれたファイル:ファイルを開くときに検索します。
- 作成された/変更された/読み込まれたファイル

たとえば、3 番目のオプションを選択した場合、エンドポイントにダウンロードされた新しいファイルが検索され、セキュリティリスクが検出されない場合には現在の場所に残されます。この残されたファイルは、ユーザがそのファイルを開いたとき、およびユーザがそのファイルを変更した場合は変更内容が保存される前に、検索されます。

検索対象ファイル

次のオプションから選択します。

- 検索可能なすべてのファイル: すべてのファイルを検索します。
- トレンドマイクロの推奨設定で検索されたファイルタイプ: 不正コードが含まれている可能性のあるファイルのみを検索します。これには無害な拡張子名で偽装されたファイルも含まれます。

  詳細については、828 ページの「トレンドマイクロの推奨設定」を参照してください。
- 対象の拡張子の選択: 拡張子がファイル拡張子リストに含まれているファイルのみを検索します。新しい拡張子を追加するか、既存の任意の拡張子を削除します。

検索設定

次のオプションから選択します (複数可)。

- シャットダウン時にフロッピーディスク検索:エンドポイントをシャットダウンする前に、フロッピーディスクでシステム領域感染型ウイルスをリアルタイム検索で検索します。これにより、ユーザがディスクからエンドポイントを再起動するときに、ウイルス/不正プログラムが実行されるのを防止します。

- 隠しフォルダの検索:手動検索時に、エンドポイント内の隠しフォルダの検出および検索を許可します。
- ネットワークドライブの検索:手動検索時またはリアルタイム検索時に、セキュリティエージェントエンドポイントにマップされたネットワークドライブやフォルダを検索します。
- 挿入後に USB ストレージデバイスのシステム領域を検索:ユーザが USB ストレージデバイスを挿入するたびに、USB ストレージデバイスのシステム領域のみを自動的に検索します (リアルタイム検索)。
- リムーバブルストレージデバイスの接続後、その中のすべてのファイルを検索:ユーザが USB ストレージデバイスを挿入するたびに、USB ストレージデバイスのすべてのファイルを自動的に検索します (リアルタイム検索)。
- メモリから検出された不正プログラムの変種を隔離:挙動監視がシステムメモリに不審プロセスがないか検索し、リアルタイム検索がそのプロセスをマップして不正プログラムがないかを検索します。不正プログラムが存在する場合、リアルタイム検索はそのプロセスまたはファイルを隔離します。

注意

- この機能を使用するには、管理者が不正変更防止サービスと高度な保護サービスを有効にしている必要があります。
- 挙動監視機能では、メモリ検索と脆弱性対策が連動して、ファイルレス攻撃に対する高度な保護を実現します。

- 圧縮ファイルの検索:Apex One では指定された圧縮階層数まで検索でき、その数を超える階層の検索はスキップできます。また、圧縮ファイル内の感染ファイルでウイルスを駆除したり、感染ファイルを削除したりします。たとえば、最大階層数が 2 の場合、検索対象の圧縮ファイルに 6 階層あったとすると、2 階層のみが検索され、残りの 4 階層の検索はスキップされます。圧縮ファイルにセキュリティ上の脅威が含まれている場合、そのファイルは駆除または削除されます。

注意

Apex One では、Office Open XML 形式の Microsoft Office 2007 ファイルは、圧縮ファイルとして扱われます。Office Open XML は Office 2007 アプリケーション用のファイル形式であり、ZIP 圧縮技術を使用しています。これらのアプリケーションを使用して作成されたファイルをウイルス/不正プログラムの検索対象にする場合、圧縮ファイルの検索を有効にする必要があります。

- OLE オブジェクトの検索:ファイルに複数の OLE 階層が含まれる場合に、指定された数の階層の検索を実行し、残りの階層は無視します。

  サーバの管理対象となるすべてのエージェントは、手動検索、リアルタイム検索、予約検索、および ScanNow の実行時に、この設定をチェックします。各層では、ウイルス/不正プログラムおよびスパイウェア/グレーウェアが検索されます。

  例:

  層数として 2 を指定した場合、あるファイルの中に Microsoft Word ドキュメント (第 1 層) が埋め込まれており、この Word ドキュメントの中に Microsoft Excel 表計算ファイルがあり (第 2 層)、さらにこの表計算ファイルの中に `.exe` ファイル (第 3 層) があるとすると、Apex One は、Word ドキュメントと Excel 表計算ファイルを検索しますが、`.exe` ファイルは検索しません。

  - OLE ファイル内の攻撃コードを検出:OLE セキュリティホールの検出では、Microsoft Office ファイルの攻撃コードを確認することで不正プログラムをヒューリスティックに特定します。

    注意

    指定した階層数は、[OLE オブジェクトの検索] オプションと [OLE ファイル内の攻撃コードを検出] オプションの両方に適用可能です。

- IntelliTrap を有効にする:圧縮された実行可能ファイルでウイルス/不正プログラムを検出および削除します。このオプションは、リアルタイム検索に対してのみ使用できます。

  詳細については、828 ページの「IntelliTrap」を参照してください。

- Web およびメールからダウンロードしたファイルに対する CVE セキュリティホールの検索を有効にする: 共通脆弱性識別子 (CVE) システムに基づいて、市販の製品の既知の脆弱性を悪用するプロセスをブロックします。このオプションは、リアルタイム検索に対してのみ使用できます。
- システム領域の検索:手動検索、予約検索、および ScanNow の実行時に、ハードディスクのシステム領域でウイルス/不正プログラムを検索します。

CPU 使用率

Apex One では、あるファイルを検索した後、次のファイルを検索する前に一時停止することができます。この設定は、手動検索、予約検索、および ScanNow の際に使用します。

次のオプションから選択します。

- 高:間隔をあけず連続してファイルを検索する
- 中:CPU 使用率が 50%を超える場合はファイル検索の合間に一時中断して間隔を空け、50%以下の場合は一時中断しない
- 低:CPU 使用率が 20%を超える場合はファイル検索の合間に一時中断して間隔を空け、20%以下の場合は一時中断しない

[中] または [低] を選択した場合、検索の開始時に CPU 使用率がしきい値 (50% または 20%) 以内の場合、検索は一時中断されず、検索時間が短縮されます。Apex One が処理で使用する CPU リソースは増えますが、CPU 使用率は最適化されているため、エンドポイントのパフォーマンスにはそれ程影響しません。CPU 使用率がしきい値を超えた時点で、Apex One は、一時中断して CPU 使用率を低下させます。再度使用率がしきい値の範囲内になると一時中断を終了します。

[高] を選択した場合、Apex One は実際の CPU 使用率をチェックせず、一時中断しないでファイルを検索します。

スケジュール

予約検索を実行する頻度 (毎日、毎週、毎月) や時刻を設定します。

月次の予約検索では、特定の日付を選択することも、曜日とその実行パターンをあわせて選択することもできます。

- 特定の日付を選択する場合: 1〜31 日の間の日付を選択します。29 日、30 日、31 日を選択した場合、これらの日付がない月では、その月の最終日に予約検索が実行されます。したがって次のようになります。
  - 29 日を選択した場合、(うるう年を除いて) 2 月は 28 日に、その他のすべての月では 29 日に予約検索が実行されます。
  - 30 日を選択した場合、2 月は 28 日または 29 日に、その他のすべての月では 30 日に予約検索が実行されます。
  - 31 日を選択した場合、2 月は 28 日または 29 日に、4 月、6 月、9 月、11 月は 30 日に、その他のすべての月では 31 日に予約検索が実行されます。
- 曜日とその実行パターンを選択した場合: 特定の曜日は各月に 4〜5 回あります。たとえば、月曜日は一般に各月 4 回あります。特定の曜日を選択して、各月の実行パターンを指定します。たとえば、各月の第 2 月曜日に予約検索を実行するように選択できます。各月の第 5 月曜日を選択した場合、第 5 月曜日に該当する日付がない月では、第 4 月曜日に予約検索が実行されます。

検索除外

検索除外を設定すると、検索パフォーマンスを向上させ、誤った警告の原因となるファイルの検索を除外させることができます。特定の種類の検索を実行するときに、Apex One は検索除外リストをチェックして、ウイルス/不正プログラムおよびスパイウェア/グレーウェアの両方の検索から除外するエンドポイント内のファイルを決定します。

検索除外を有効にすると、次の条件を満たすファイルは検索されません。

- 特定のディレクトリ (またはそのサブディレクトリ) 内にあるファイル。
- ファイル名が除外リストにあるいずれかの名前と一致するもの。
- ファイル拡張子が除外リストにあるいずれかの拡張子と一致するもの。

ヒント

リアルタイム検索の対象から除外することが推奨される製品のリストについては、次を参照してください。

https://success.trendmicro.com/jp/solution/1313316

ワイルドカードによる除外設定

ファイルとディレクトリに対する検索除外リストでは、ワイルドカード文字を使用できます。「?」は任意の 1 文字を表し、「*」は任意の文字列を表します。

ワイルドカード文字は慎重に使用してください。間違った文字を使用すると、意図しないファイルやディレクトリが除外されることがあります。たとえば、C:¥*を検索除外リスト (ファイル) に追加すると、C:¥ドライブ全体が除外されます。

表 7-11. ワイルドカード文字を使用した検索除外

値	除外されるもの	除外されないもの
c:\director*\fil*.txt	c:¥directory¥fil¥doc.txt c:¥directories¥fil¥files¥document.txt	c:¥directory¥file¥ c:¥directories¥files¥ c:¥directory¥file¥doc.txt c:¥directories¥files¥document.txt
c:\director?\file*.txt	c:¥directory¥file¥doc.txt	c:¥directories¥file¥document.txt
c:\director?\file\?.txt	c:¥directory¥file¥1.txt	c:¥directory¥file¥doc.txt c:¥directories¥file¥document.txt
c:*.txt	C:¥ディレクトリ内のすべての.txt ファイル	C:¥ディレクトリ内のその他のすべてのファイルタイプ
[]	サポートされていません	サポートされていません

検索除外リスト (ディレクトリ)

Apex One は、コンピュータ上の特定のディレクトリにあるすべてのファイルを検索しなくなります。最大 256 ディレクトリを指定できます。

注意

ディレクトリを検索から除外することによって、Apex One は自動的にそのディレクトリのすべてのサブディレクトリも検索から除外します。

[トレンドマイクロ製品がインストールされているディレクトリの除外] を選択することもできます。このオプションを選択すると、次のトレンドマイクロ製品のディレクトリが検索から自動的に除外されます。

- <サーバインストールフォルダ>

  注意

  手動検索の場合、除外後もサーバインストールフォルダは検索されます。

- IM Security
- InterScan eManager 3.5x
- InterScan Web Security Suite
- InterScan Web Protect
- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan NSAPI Plug-in
- InterScan E-mail VirusWall
- InterScan eManager 3.11、5.1、5.11、5.12
- InterScan for Lotus Notes eManager NT
- InterScan for Microsoft Exchange

リストにないトレンドマイクロ製品を使用している場合には、その製品ディレクトリを検索除外リストに追加します。

さらに、[エージェント] > [グローバルエージェント設定] の [セキュリティ設定] タブにある [検索設定] セクションに移動し、Microsoft Exchange 2000/2003 ディレクトリを除外するように設定します。Microsoft Exchange 2007 以降を使用している場合は、該当するディレクトリを検索除外リストに手動で追加します。検索除外の詳細については、次のサイトを参照してください。

http://technet.microsoft.com/ja-jp/library/bb332342.aspx

ファイルリストの設定時には、次のオプションのいずれかを選択します。

- 現在のリストを維持 (初期設定): このオプションは、エージェントの既存の除外リストが間違って上書きされるのを防止します。除外リストに加えた変更を保存して適用する場合は、これ以外のオプションを選択してください。
- 上書き: このオプションは、エージェント上の除外リスト全体を削除し、現在のリストで置き換えます。[すべてのエージェントに適用] をクリックすると、確認の警告メッセージが表示されます。
- パスを追加: このオプションは、現在のリスト内の項目をエージェントの既存の除外リストに追加します。エージェントの除外リストにすでに存在する項目は無視されます。
- パスを削除: このオプションは、現在のリスト内の項目がエージェントの既存の除外リストにあった場合、既存のリストからその項目を削除します。

検索除外リスト (ディレクトリ) のサポート対象のシステム変数

Windows の一般的なシステム変数を使用して、ディレクトリの検索除外リストを設定できます。次の表は、Apex One でサポートされる変数を示しています。

システム変数	説明
%ALLUSERSPROFILE%	%PROFILESFOLDER%¥Public フォルダまたは%PROFILESFOLDER%¥all users フォルダを参照します。 例を以下に示します。 • Windows 7 における%ALLUSERSPROFILE%の初期設定の場所: C:¥ProgramData
%COMMONPROGRAMFILES(X86)%	64 ビットシステム上の C:¥Program Files (x86)¥Common Files フォルダを参照します。
%PROGRAMFILES%	Program Files フォルダ 標準のパスは C:¥Program Files です。
%PROGRAMFILES(X86)%	64 ビットシステム上の C:¥Program Files (x86) フォルダを参照します。
%SYSTEMROOT%	システムドライブのルートを参照します。 標準のパスは C:¥Windows です。
%WINDIR%	システムドライブにある Windows フォルダを参照します。 標準のパスは C:¥Windows です。

検索除外リスト (ファイル)

Apex One は、この除外リストに含まれているいずれかのファイル名に一致するファイルがある場合、そのファイルを検索しません。エンドポイント上の特定の場所にあるファイルを除外する場合は、C:¥Temp¥sample.jpg のようにファイルパスを含めて指定します。

最大 256 ファイルを指定できます。

ファイルリストの設定時には、次のオプションのいずれかを選択します。

- 現在のリストを維持 (初期設定): このオプションは、エージェントの既存の除外リストが間違って上書きされるのを防止します。除外リストに加

えた変更を保存して適用する場合は、これ以外のオプションを選択してください。

- 上書き: このオプションは、エージェント上の除外リスト全体を削除し、現在のリストで置き換えます。[すべてのエージェントに適用] をクリックすると、確認の警告メッセージが表示されます。
- パスを追加: このオプションは、現在のリスト内の項目をエージェントの既存の除外リストに追加します。エージェントの除外リストにすでに存在する項目は無視されます。
- パスを削除: このオプションは、現在のリスト内の項目がエージェントの既存の除外リストにあった場合、既存のリストからその項目を削除します。

検索除外リスト (ファイル拡張子)

Apex One は、この除外リストに含まれているいずれかのファイル拡張子に一致するファイルがある場合、そのファイルを検索しません。最大 256 のファイル拡張子を指定できます。拡張子の前にピリオド (.) を付ける必要はありません。

手動検索、予約検索、および ScanNow の場合、ワイルドカード文字として疑問符 (?) を使用して 1 つの文字を置き換えるか、アスタリスク (*) を使用して複数の文字を置き換えます。たとえば、DOC、DOT、DAT など、D で始まる拡張子を持つすべてのファイルを検索しない場合は、「`D*`」または「`D??`」と入力します。

注意

リアルタイム検索では、拡張子を指定するときにワイルドカードは使用できません。

すべての検索タイプに検索除外設定を適用する

Apex One では、特定の検索の種類に対して検索除外設定を行い、同じ設定を他のすべての検索の種類に適用することができます。次に例を示します。

1 月 1 日に、Apex One 管理者の Chris が、エージェントコンピュータに大量の JPG ファイルがあることを見つけて、これらのファイルにセキュリティ上

の脅威がないことを確認しました。Chris は、手動検索のファイル除外リストに JPG を追加し、次にこの設定をすべての検索の種類に適用しました。これにより、リアルタイム検索、ScanNow、および予約検索は、.jpg ファイルの検索をスキップするように設定されました。

1 週間後、Chris は、リアルタイム検索の除外リストから JPG を削除しましたが、すべての検索の種類には検索除外の設定を適用しませんでした。これにより、JPG ファイルはリアルタイム検索の場合にのみ検索されるようになります。

検出時の処理

特定の検索の種類でセキュリティリスクを検出したときに、Apex One が実行する処理を指定します。選択できる検出時の処理は、ウイルス/不正プログラムとスパイウェア/グレーウェアで異なります。

ウイルス/不正プログラムの検出時の処理

実行される処理は、ウイルス/不正プログラムの種類と、これらを検出した検索の種類によって異なります。たとえば、手動検索 (検索の種類) によってトロイの木馬プログラム (ウイルス/不正プログラムの種類) が検出された場合は、感染ファイルが駆除 (処理) されます。

ウイルス/不正プログラムの種類については、272 ページの「ウイルスと不正プログラム」を参照してください。

Apex One がウイルス/不正プログラムに対して実行可能な処理は次のとおりです。

表 7-12. ウイルス/不正プログラムの検出時の処理

処理	説明
削除	Apex One では、感染したファイルを削除します。

処理	説明
隔離	Apex One では、感染ファイルの名前を変更および暗号化し、エージェントエンドポイントの一時隔離ディレクトリである<エージェントインストールフォルダ>¥Suspect に検出された感染ファイルを移動します。 セキュリティエージェントでは、指定された隔離ディレクトリに隔離ファイルを送信します。 詳細については、312 ページの「隔離ディレクトリ」を参照してください。 初期設定の隔離ディレクトリの場所は、Apex One サーバの<サーバインストールフォルダ>¥PCCSRV¥Virus です。 隔離されたファイルを復元する必要がある場合には、隔離の一括復元機能を使用します。 詳細については、316 ページの「隔離ファイルの復元」を参照してください。
駆除	Apex One では、感染ファイルへのフルアクセスを許可する前に駆除します。 ファイルを駆除できない場合、Apex One では 2 次処理を実行します。2 次処理として実行できるのは、隔離、削除、拡張子変更、または放置 (ログのみ) のいずれかです。 2 次処理を設定するには、[エージェント] > [エージェント管理] に移動します。さらに、[設定] > [検索設定] > {検索の種類} > [処理] タブの順にクリックします。 この処理は、潜在的なウイルス/不正プログラムを除くすべての種類の不正プログラムに対して実行できます。
拡張子変更	Apex One では、感染ファイルの拡張子を「vir」に変更します。拡張子が変更されたファイルはそのままでは開くことはできませんが、特定のアプリケーションに関連付けると開くことができます。 拡張子を変更した感染ファイルを開くと、ウイルス/不正プログラムが作動する可能性があります。
放置	Apex One では、手動検索、予約検索、および ScanNow を実行中に、いずれかの種類のウイルスが検出された場合のみ、この検出時処理を使用できます。感染ファイルを開いたり実行したりする操作が検出されたときに何も処理を実行しないとウイルス/不正プログラムが実行されてしまうため、リアルタイム検索中はこの処理は使用できません。他の処理は、すべてリアルタイム検索中に使用できます。

処理	説明
アクセス拒否	この検出時の処理は、リアルタイム検索の場合にのみ実行可能です。感染ファイルを開こうとしたり実行しようとする操作が検出された場合、その操作は即座にブロックされます。 ユーザは感染ファイルを手動で削除できます。

トレンドマイクロの推奨処理を使用

ウイルス/不正プログラムの種類ごとに、異なる検索処理が必要になります。検索処理のカスタマイズには、ウイルス/不正プログラムに関する知識が必要であり、時間と手間のかかる作業になる可能性があります。トレンドマイクロの推奨処理を使用して、この問題に対応することが可能です。

トレンドマイクロの推奨処理とは、ウイルス/不正プログラムに事前に割り当てられている一連の検索処理です。検索処理について詳しくない場合や、ウイルス/不正プログラムに適した検索処理の判断が難しい場合は、トレンドマイクロの推奨処理をお勧めします。

トレンドマイクロの推奨処理を使用する利点は、次のとおりです。

- トレンドマイクロの推奨処理では、トレンドマイクロが推奨する検索処理が使用されます。検出時の処理を設定する手間が省けます。
- ウイルス作成者は、ウイルス/不正プログラムによる攻撃手段を絶えず変えています。トレンドマイクロの推奨処理の設定は、最新の脅威やウイルス/不正プログラムの最新の攻撃手段に対応して保護できるように更新されます。

注意

トレンドマイクロの推奨処理は、スパイウェア/グレーウェア検索には使用できません。

次の表は、ウイルス/不正プログラムの種類に応じて適用されるトレンドマイクロの推奨処理を示しています。

表 7-13. ウイルス/不正プログラムに適用されるトレンドマイクロの推奨処理

ウイルスや不正プログラム	リアルタイム検索		手動検索/予約検索/ScanNow	
	1 次処理	2 次処理	1 次処理	2 次処理
CVE セキュリティホール	アクセス拒否	該当なし	該当なし	該当なし
ジョークプログラム	隔離	該当なし	隔離	該当なし
トロイの木馬	隔離	該当なし	隔離	該当なし
ウイルス	駆除	隔離	駆除	隔離
テストウイルス	アクセス拒否	該当なし	放置	該当なし
パッカー	隔離	該当なし	隔離	該当なし
潜在的な不正プログラム	アクセス拒否またはユーザ設定の処理	該当なし	放置(ログのみ)またはユーザ設定の処理	該当なし
その他の不正プログラム	駆除	隔離	駆除	隔離

潜在的な不正プログラムの場合、リアルタイム検索の初期設定の処理は「アクセス拒否」、手動検索、予約検索、および ScanNow の初期設定の処理は「放置 (ログのみ)」です。これらが適切な処理ではない場合、隔離、削除、拡張子変更などに変更できます。

すべての種類のウイルス/不正プログラムに同じ処理を使用

このオプションは、潜在的なウイルス/不正プログラムを除くすべての種類のウイルス/不正プログラムに同じ処理を実行する場合に選択します。1 次処理として「駆除」を選択した場合、駆除に失敗した場合に実行する 2 次処理を選択します。1 次処理が「駆除」ではない場合、2 次処理を設定することはできません。

1 次処理に「駆除」を選択した場合、潜在的なウイルス/不正プログラムが検出されたときに 2 次処理が実行されます。

特定の処理を検出されたウイルス/不正プログラムの種類ごとに使用

ウイルス/不正プログラムの種類ごとに検索時の処理を手動で選択します。

潜在的なウイルス/不正プログラム以外のウイルス/不正プログラムには、すべての検出時の処理を使用できます。1 次処理として「駆除」を選択した場合、駆除に失敗した場合に実行する 2 次処理を選択します。1 次処理が「駆除」ではない場合、2 次処理を設定することはできません。

潜在的なウイルス/不正プログラムの場合、「駆除」以外のすべての検出時の処理を使用できます。

隔離ディレクトリ

感染ファイルの処理が「隔離」の場合、セキュリティエージェントはそのファイルを暗号化し、<エージェントインストールフォルダ>¥SUSPECT にある一時隔離フォルダに移動します。次に、指定された隔離ディレクトリにファイルを送信します。

注意

暗号化された隔離ファイルにアクセスする必要がある場合には、そのファイルを復元することができます。

詳細については、318 ページの「暗号化ファイルの復元」を参照してください。

初期設定の隔離ディレクトリをそのまま使用します。このディレクトリは Apex One サーバコンピュータに配置され、サーバのホスト名または IP アドレスを含む URL の形式で指定されます。

- サーバが IPv4 と IPv6 の両方のエージェントを管理している場合は、すべてのセキュリティエージェントが隔離ファイルをサーバに送信できるようにホスト名を使用してください。
- サーバの識別に IPv4 アドレスのみが使用されている場合、サーバに隔離ファイルを送信できるのは、IPv4 シングルスタックセキュリティエージェントとデュアルスタックエージェントのみです。

- サーバの識別に IPv6 アドレスのみが使用されている場合、サーバに隔離ファイルを送信できるのは、IPv6 シングルスタックセキュリティエージェントとデュアルスタックエージェントのみです。

URL、UNC パス、あるいは絶対ファイルパスの形式で、別の隔離ディレクトリを指定することもできます。セキュリティエージェントから接続可能なディレクトリを指定する必要があります。たとえば、この代替ディレクトリがデュアルスタックセキュリティエージェントおよび IPv6 シングルスタックエージェントから隔離ファイルを受信する場合は、ディレクトリに IPv6 アドレスが割り当てられている必要があります。代替ディレクトリにはデュアルスタックディレクトリを指定し、ホスト名でそのディレクトリを識別して、ディレクトリを入力する際には UNC パスを使用することをお勧めします。

次の表は、URL、UNC パス、または絶対ファイルパスを使用する状況について説明しています。

表 7-14. 隔離ディレクトリ

隔離ディレクトリ	使用可能な形式	例	備考
管理サーバコンピュータのディレクトリ	URL	`http://<osceserver>`	これは初期設定のディレクトリです。 隔離フォルダのサイズなど、このディレクトリの設定を行います。 詳細については、632 ページの「隔離フォルダ設定」を参照してください。
	UNC パス	`¥¥<osceserver>¥ofcscan¥Virus`	

隔離ディレクトリ	使用可能な形式	例	備考
他の Apex One サーバコンピュータのディレクトリ (ネットワーク上に他の Apex One サーバがある場合)	URL	`http://<osceserver2>`	セキュリティエージェントがこのディレクトリに接続可能であることを確認します。間違ったディレクトリを指定した場合、セキュリティエージェントは正しい隔離ディレクトリが指定されるまで、\Suspect フォルダに隔離ファイルを保存します。サーバのウイルス/不正プログラムログには、隔離ファイルを指定された隔離フォルダに移動できなかったことが記録されます。 UNC パスを使用している場合、隔離ディレクトリフォルダが「Everyone」グループで共有されていることと、このグループに対して読み取り/書き込み許可を割り当てていることを確認してください。
	UNC パス	`¥¥<osceserver2>¥ofcscan¥Virus`	
ネットワーク上の別のエンドポイント	UNC パス	`¥¥<computer_name>¥temp`	
セキュリティエージェントの別のディレクトリ	絶対パス	`C:¥temp`	

ウイルス駆除実行前にバックアップを作成

Apex One が感染ファイルを駆除するように設定されている場合、最初にファイルをバックアップすることができます。これにより、後でこのファイルが必要になった場合にファイルを復元できます。Apex One によってバックアップファイルは開かれないように暗号化され、<エージェントインストールフォルダ>¥Backup フォルダに保存されます。

暗号化されたバックアップファイルを復元する方法については、318 ページの「暗号化ファイルの復元」を参照してください。

ダメージクリーンナップサービス

ダメージクリーンナップサービスは、ファイルベースのコンピュータウイルス、ネットワークウイルス、およびウイルスやワームの残骸 (トロイの木馬、レジストリ侵入、ウイルスファイル) を駆除します。

エージェントでは、ダメージクリーンナップサービスが検索の種類に応じて、ウイルス/不正プログラムの検索の前または後に実行されます。

- 手動検索、予約検索、または ScanNow の実行時、セキュリティエージェントではダメージクリーンナップサービスが実行されてから、ウイルス/不正プログラムの検索に進みます。ウイルス/不正プログラムの検索時にクリーンナップが要求された場合は、ダメージクリーンナップサービスをもう一度実行できます。
- リアルタイム検索時にセキュリティエージェントでクリーンナップが要求された場合は、先にウイルス/不正プログラムの検索が実行され、次にダメージクリーンナップサービスが実行されます。

ダメージクリーンナップサービスを実行するクリーンナップの種類を選択できます。

- 標準クリーンナップ: セキュリティエージェントでは、標準クリーンナップの間に次のいずれかの処理が実行されます。
  - 活動中のトロイの木馬を検出および削除
  - トロイの木馬が作成したプロセスを中止
  - トロイの木馬が変更したシステムファイルを修復
  - トロイの木馬により作成されたファイルとアプリケーションを削除
- 高度なクリーンナップ:標準クリーンナップの処理の他に、セキュリティエージェントでは、FakeAV と呼ばれる偽セキュリティソフトウェアや特定のルートキットの変種による活動が停止されます。さらに、セキュリティエージェントでは、高度なクリーンナップルールを使用して、FakeAV やルートキットの挙動を示すアプリケーションを予防的に検出および停止できます。

注意

高度なクリーンナップでは、積極的な保護を提供する一方で、誤検出の数も多くなります。

ダメージクリーンナップサービスは、[ウイルス/不正プログラムの可能性が検出された場合にクリーンナップを実行] オプションが選択されない限り、潜在的なウイルス/不正プログラムに対してクリーンナップを実行しません。この

オプションは、潜在的なウイルス/不正プログラムに対する処理が、「放置 (ログのみ)」または「アクセス拒否」以外の場合にのみ選択できます。たとえば、セキュリティエージェントでリアルタイム検索時に潜在的なウイルス/不正プログラムが検出された場合、その処理が隔離であれば、最初に感染ファイルが隔離され、次に必要に応じてクリーンナップが実行されます。クリーンナップの種類 (標準または高度) は、選択内容に従います。

ウイルス/不正プログラムの検出時に通知を表示する

Apex One では、リアルタイム検索および予約検索時にウイルス/不正プログラムを検出した場合に、検出したことをユーザに知らせる通知メッセージを表示できます。

通知メッセージを変更するには、[管理] > [通知] > [エージェント] の [種類] のドロップダウンから [ウイルス/不正プログラム] を選択します。

潜在的なウイルス/不正プログラムの検出時に通知を表示する

Apex One では、リアルタイム検索および予約検索時に潜在的なウイルス/不正プログラムを検出した場合に、検出したことをユーザに知らせる通知メッセージを表示できます。

通知メッセージを変更するには、[管理] > [通知] > [エージェント] の [種類] のドロップダウンから [ウイルス/不正プログラム] を選択します。

隔離ファイルの復元

誤検出であることが確実な場合は、隔離されたファイルを復元できます。隔離の一括復元機能を使用して、隔離ディレクトリでファイルを検索し、SHA1 による追加検証を実施して、復元するファイルが一切変更されていないことを確認できます。

手順

1. [エージェント] > [エージェント管理]に移動します。
2. エージェントツリーで、ドメインまたはエージェントを選択します。

3. [タスク] > [隔離の一括復元] の順にクリックします。

   [隔離の一括復元条件] 画面が表示されます。

4. [感染ファイル/オブジェクト] フィールドに、復元するデータの名前を入力します。

5. 必要に応じて、期間、セキュリティ上の脅威名、およびデータのファイルパスを指定します。

6. [検索] をクリックします。

   [隔離の一括復元] 画面に検索結果が表示されます。

7. ファイルを復元するドメイン内のすべてのセキュリティエージェントで、該当ファイルが検索除外リストに追加されるようにするには、[復元したファイルをドメインレベルの除外リストに追加する] を選択します。

   これにより、以降の検索でこのファイルは脅威として検出されなくなります。

   重要

   Apex Central ポリシーを使用して管理されるセキュリティエージェントは、次回 Apex Central サーバによってセキュリティエージェントポリシーが更新されて除外リストが上書きされるまで、復元したファイルの除外のみを適用します。セキュリティエージェントが復元したファイルを再検索しないようにするには、Apex Central セキュリティエージェントポリシーにファイルの除外を追加してください。

8. 必要に応じて、検証のためにファイルの SHA-1 値を入力します。

9. リストから復元するファイルを選択して、[復元] をクリックします。

   ヒント

   ファイルが復元される各セキュリティエージェントを表示するには、[エンドポイント] 列のリンクをクリックします。

10. 確認ダイアログで [閉じる] をクリックします。

隔離ファイルが正常に復元されたことを確認する方法については、370 ページの「隔離の一括復元ログの表示」を参照してください。

暗号化ファイルの復元

Apex One では、感染ファイルが開かれないように、次の時点でファイルを暗号化します。

- ファイルを隔離する前
- ファイルのウイルス駆除実行前のバックアップ時

Apex One には、ファイルから情報を取得する必要がある場合に、ファイルを復号して復元するツールが用意されています。Apex One では、次のファイルの復号および復元が可能です。

表 7-15. Apex One が復号および復元可能なファイル

ファイル	説明
エージェントエンドポイント上の隔離されたファイル	このファイルは、<エージェントインストールフォルダ>¥SUSPECT¥Backup フォルダにあり、7 日後に自動的に削除されます。また、Apex One サーバの指定された隔離ディレクトリにアップロードされます。
指定された隔離ディレクトリの隔離ファイル	初期設定では、この隔離ディレクトリは、Apex One サーバコンピュータに配置されます。 詳細については、312 ページの「隔離ディレクトリ」を参照してください。
バックアップされた暗号化ファイル	Apex One で駆除可能な感染ファイルのバックアップです。このファイルは、<エージェントインストールフォルダ>¥Backup フォルダにあります。ユーザがこのファイルを復元する場合、<エージェントインストールフォルダ>¥SUSPECT¥Backup フォルダに移動する必要があります。 Apex One では、[エージェント] > [エージェント管理] の [設定] > [検索設定] > {検索の種類} > [処理] タブで [ウイルス駆除実行前にバックアップを作成] を選択した場合にのみ、駆除前にバックアップと暗号化が実行されます。

警告!

感染ファイルを復元すると、ウイルス/不正プログラムが他のファイルやコンピュータに感染を拡大させる可能性があります。ファイルを復元する前に、感染したエンドポイントを隔離して、そのエンドポイントにある重要なファイルをバックアップの場所に移動してください。

ファイルの復号と復元

手順

- ファイルがセキュリティエージェントエンドポイントにある場合:

  a. コマンドプロンプトを開き、<エージェントインストールフォルダ>に移動します。

  b. ファイルをダブルクリックするか、コマンドプロンプトで次のコマンドを入力して、VSEncode.exe を実行します。

  ```
  VSEncode.exe /u
  ```

  このパラメータは、<エージェントインストールフォルダ>¥SUSPECT¥Backup にあるファイルのリストを画面に表示します。

  c. 復元するファイルを選択して、[復元] をクリックします。このツールで復元できるのは、一度に 1 つのファイルのみです。

  d. 表示された画面で、ファイルを復元するフォルダを指定します。

  e. [OK] をクリックします。指定されたフォルダにファイルが復元されます。

  注意

  Apex One によってファイルが再度検索され、復元後ただちにファイルが感染ファイルとして処理される場合もあります。ファイルが検索されないようにするには、そのファイルを検索除外リストに追加します。詳細については、302 ページの「検索除外」を参照してください。

  f. ファイルの復元が終了したら、[閉じる] をクリックします。

- ファイルが Apex One サーバまたはカスタム隔離ディレクトリにある場合:

  a. ファイルが Apex One サーバコンピュータにある場合は、コマンドプロンプトを開いて、<サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility¥VSEncrypt に移動します。

     ファイルがカスタム隔離ディレクトリにある場合は、<サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility に移動して、カスタム隔離ディレクトリがあるエンドポイントに VSEncrypt フォルダをコピーします。

  b. テキストファイルを作成して、暗号化または復号するファイルの完全パスを入力します。

     たとえば、C:¥My Documents¥Reports にあるファイルを復元するには、テキストファイルに「C:¥My Documents¥Reports¥*.*」と記述します。

     Apex One サーバコンピュータの隔離ファイルは、<サーバインストールフォルダ>¥PCCSRV¥Virus にあります。

  c. テキストファイルを INI または TXT の拡張子を付けて保存します。たとえば、C: ドライブに ForEncryption.ini という名前で保存します。

  d. コマンドプロンプトを開き、VSEncrypt フォルダのあるディレクトリに移動します。

  e. 次のコマンドを入力して、VSEncode.exe を実行します。

     ```
     VSEncode.exe /d /i <INI または TXT ファイルのパス>
     ```

     説明:

     <INI または TXT ファイルのパス> は、作成した INI または TXT ファイルのパスです (例: C:¥ForEncryption.ini)。

  f. その他のパラメータを使用して、さまざまなコマンドを実行できます。

表 7-16. 復元パラメータ

パラメータ	説明
なし (パラメータなし)	ファイルを暗号化します。
/d	ファイルを復号します。
/debug	デバッグログを作成し、エンドポイントに保存します。セキュリティエージェントエンドポイントの <エージェントインストールフォルダ> に、デバッグログ (VSEncrypt.log) が作成されます。
/o	暗号化または復号されたファイルがすでに存在する場合に、そのファイルを上書きします。
/f <ファイル名>	1 つのファイルを暗号化または復号します。
/nr	元のファイル名を復元しません。
/v	ツールに関する情報を表示します。
/u	ツールのユーザインタフェースを起動します。
/r <復元先フォルダ>	ファイルを復元するフォルダ
/s <元のファイル名>	暗号化された元のファイルのファイル名

たとえば、「VSEncode [/d] [/debug]」と入力して、Suspect フォルダ内のファイルを復号し、デバッグログを作成します。ファイルを復号または暗号化すると、Apex One によって同じフォルダに復号または暗号化されたファイルが作成されます。ファイルを復号または暗号化する前に、ロックされていないことを確認してください。

スパイウェア/グレーウェアの検出時の処理

実行される検出時の処理は、スパイウェア/グレーウェアを検出した検索の種類によって異なります。ウイルス/不正プログラムの種類ごとに特定の処理を設定できますが、すべての種類のスパイウェア/グレーウェアに対して 1 つの処理のみを設定することもできます。たとえば、手動検索 (検索の種類) によっていずれかのスパイウェア/グレーウェアが検出された場合は、影響を受けたシステムリソースが駆除 (処理) されます。

各種のスパイウェア/グレーウェアについては、275 ページの「スパイウェアとグレーウェア」を参照してください。

注意

スパイウェア/グレーウェアの検出時の処理は、Web コンソールでのみ設定可能です。セキュリティエージェントコンソールからはこれらの設定にアクセスできません。

Apex One がスパイウェア/グレーウェアに対して実行可能な処理は次のとおりです。

表 7-17. スパイウェア/グレーウェアの検出時の処理

処理	説明
駆除	プロセスを終了するか、レジストリ、ファイル、Cookie、およびショートカットを削除します。 スパイウェア/グレーウェアを駆除した後、セキュリティエージェントでスパイウェア/グレーウェアのデータをバックアップし、スパイウェア/グレーウェアに安全にアクセスできると考えられる場合、復元することができます。 詳細については、325 ページの「スパイウェア/グレーウェアの復元」を参照してください。
放置	検出されたスパイウェア/グレーウェアコンポーネントには処理は実行されません。ただし、スパイウェア/グレーウェア検出のログが記録されます。 検出されたスパイウェア/グレーウェアが承認済みリストに含まれている場合、いずれの処理も実行されません。 詳細については、323 ページの「スパイウェア/グレーウェアの承認済みリスト」を参照してください。
アクセス拒否	検出されたスパイウェア/グレーウェアコンポーネントへのアクセス (コピー、開く) を拒否します。この処理は、リアルタイム検索の場合にのみ実行可能です。手動検索、予約検索、および ScanNow の場合は、処理が「放置(ログのみ)」になります。

スパイウェア/グレーウェアの検出時に通知を表示する

Apex One では、リアルタイム検索および予約検索時にスパイウェア/グレーウェアを検出した場合に、検出したことをユーザに知らせる通知メッセージを表示できます。

通知メッセージを変更するには、[管理] > [通知] > [エージェント] の [種類] のドロップダウンから [スパイウェア/グレーウェア] を選択します。

スパイウェア/グレーウェアの承認済みリスト

セキュリティエージェントには、「承認済み」のスパイウェア/グレーウェアのリストが用意されています。このリストには、スパイウェアまたはグレーウェアとして処理しないファイルまたはアプリケーションが含まれます。検索時に特定のスパイウェア/グレーウェアが検出されると、セキュリティエージェントではこの承認済みリストをチェックし、リスト内に一致する項目がある場合は処理を実行しません。

承認済みリストを、1 つ以上のセキュリティエージェントおよびドメインに適用するか、またはサーバが管理するすべてのセキュリティエージェントに適用します。承認済みリストをすべての検索の種類に適用するということは、手動検索、リアルタイム検索、予約検索、および ScanNow の際に同じ承認済みリストを使用するということを意味します。

検出済みのスパイウェア/グレーウェアの承認済みリストへの追加

手順

1. 次のいずれかに移動します。
   - [エージェント] > [エージェント管理]
   - [ログ] > [エージェント] > [セキュリティリスク]
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。

3. [ログ] > [スパイウェア/グレーウェアログ] または [ログの表示] > [スパイウェア/グレーウェアログ] をクリックします。
4. ログの条件を指定して [ログを表示する] をクリックします。
5. ログを選択して、[承認済みリストに追加] をクリックします。
6. 承認済みスパイウェア/グレーウェアを、選択したエージェントコンピュータのみに適用するか、特定のドメインに適用します。
7. [保存]をクリックします。選択したエージェントに設定が適用され、[エージェント] > [エージェント管理] > [設定] > [スパイウェア/グレーウェアの承認済みリスト] の承認済みリストに、Apex One サーバによってスパイウェア/グレーウェアが追加されます。

注意

Apex One では、最大 1024 のスパイウェア/グレーウェアを承認済みリストに追加できます。

スパイウェア/グレーウェアの承認済みリストの管理

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [スパイウェア/グレーウェアの承認済みリスト] の順にクリックします。
4. [スパイウェア名] テーブルで、スパイウェア/グレーウェア名を選択します。複数の名前を選択するには、<Ctrl> キーを押しながら選択します。
   - また、[検索] にキーワードを入力して、[検索開始] をクリックすることもできます。キーワードに一致する名前でテーブルが更新されます。

5. [追加] をクリックします。

   これらの名前が [承認済みリスト] テーブルに移動します。

6. 承認済みリストから名前を削除するには、名前を選択して [削除] をクリックします。複数の名前を選択するには、<Ctrl> キーを押しながら選択します。

7. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。

   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
   - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

スパイウェア/グレーウェアの復元

スパイウェア/グレーウェアの駆除後、セキュリティエージェントはスパイウェア/グレーウェアのデータをバックアップします。データが無害であると考えられる場合は、オンラインエージェントにバックアップされたデータを復元するように通知します。バックアップ時間に基づいて復元するスパイウェア/グレーウェアのデータを選択します。

注意

セキュリティエージェントのユーザは、スパイウェア/グレーウェアの復元を開始することができません。また、エージェントで復元できたバックアップデータについて通知されません。

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーでドメインを開き、エージェントを選択します。

   注意

   一度にスパイウェア/グレーウェアの復元を実行できるエージェントは 1 つのみです。

3. [タスク] > [スパイウェア/グレーウェアの復元] の順にクリックします。
4. 復元するアイテムをデータセグメントごとに表示するには、[表示] をクリックします。

   新しい画面が表示されます。[戻る] をクリックして前の画面に戻ります。
5. 復元するデータセグメントを選択します。
6. [復元] をクリックします。

   復元のステータスが通知されます。完全なレポートについては、スパイウェア/グレーウェアの復元ログを確認してください。詳細については、375 ページの「スパイウェア/グレーウェア復元ログの表示」を参照してください。

信頼済みプログラムリスト

アプリケーションコントロール、挙動監視、デバイスコントロール、Endpoint Sensor、およびリアルタイム検索で信頼済みプロセスの検索を省略するようにセキュリティエージェントを設定できます。信頼済みプログラムリストにプログラムを追加すると、そのプログラムとそのプログラムによって開始されたプロセスはリアルタイム検索の対象から除外されます。信頼するプログラムをリストに追加すると、エンドポイントの検索パフォーマンスが向上します。

注意

信頼済みプログラムリストに追加できるのは、次の要件を満たすファイルです。

- Windows システムディレクトリに格納されていない。
- 有効なデジタル署名がある。

信頼済みプログラムリストに追加したプログラムは、以降、次の検索の対象から自動的に除外されます。

- アプリケーションコントロール (Apex Central コンソールでのみ設定可能)
- 挙動監視
- デバイスコントロール
- Endpoint Sensor (Apex Central コンソールでのみ設定可能)
- リアルタイム検索: ファイルチェックとプロセス検索

信頼済みプログラムリストの設定

信頼済みプログラムリストは、プログラムとそのプログラムで呼び出されるすべての子プロセスをアプリケーションコントロール、挙動監視、デバイスコントロール、Endpoint Sensor、およびリアルタイム検索から除外します。

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [信頼済みプログラムリスト] の順にクリックします。
4. 検索から除外するプログラムのフルパスを入力します。
5. [信頼済みプログラムリストに追加] をクリックします。

6. リストからプログラムを削除するには、[削除] アイコンをクリックします。
7. 信頼済みプログラムリストをエクスポートするには、[エクスポート] をクリックしてファイルの場所を選択します。

   注意

   リストが DAT 形式で保存されます。

8. 信頼済みプログラムリストをインポートするには、[インポート] をクリックしてファイルの場所を選択します。
   a. [参照...] をクリックして、DAT ファイルの場所を選択します。
   b. [インポート] をクリックします。
9. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。
   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
   - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

検索権限とその他の設定

検索権限のあるユーザは、コンピュータ上のファイルの検索方法をより詳細に制御できます。検索権限を持つユーザまたはセキュリティエージェントは、次の操作を実行できます。

- ユーザは、手動検索、予約検索、およびリアルタイム検索を設定できます。詳細については、329 ページの「検索の種類権限」を参照してください。

- ユーザは、予約検索を延期、停止、またはスキップできます。詳細については、330 ページの「予約検索権限とその他の設定」を参照してください。
- ユーザは、POP3 メールメッセージでのウイルス/不正プログラムの検索を有効化できます。詳細については、334 ページの「メール検索権限とその他の設定」を参照してください。
- セキュリティエージェントは、キャッシュ設定を使用して、検索のパフォーマンスを向上できます。詳細については、336 ページの「検索用のキャッシュ設定」を参照してください。
- ユーザは、個々の信頼済みプログラムリストをカスタマイズできます。詳細については、340 ページの「信頼済みプログラムリスト権限」を参照してください。

検索の種類権限

ユーザに、手動検索、リアルタイム検索、および予約検索の独自の設定を行う権限を付与します。

検索の種類権限の付与

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [権限] タブの [検索] セクションに移動します。
5. ユーザに設定を許可する検索の種類を選択します。
6. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。

- すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
- 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

セキュリティエージェントの検索設定

手順

1. タスクトレイの [セキュリティエージェント] アイコンを右クリックして、[セキュリティエージェントコンソールの起動] を選択します。
2. [設定] > {検索の種類} の順にクリックします。
3. 次の設定を行います。
   - リアルタイム検索:検索するファイル、検出時の処理、検索除外、詳細設定
   - 手動検索: 検索するファイル、検出時の処理、検索除外、詳細設定
   - 予約検索: 予約検索を有効にする、検索頻度、検索するファイル、検出時の処理、検索除外、詳細設定
4. [OK] をクリックします。

予約検索権限とその他の設定

予約検索がエージェントで実行するよう設定されている場合、ユーザが予約検索を延期およびスキップ/停止できます。

予約検索の延期

「予約検索の延期」権限を持つユーザは、次の処理を実行できます。

- 予約検索を実行する前にそれを延期させて、その延期期間を指定できます。予約検索は一度だけ延期できます。
- 予約検索が実行されている場合、ユーザは検索を停止して後で再開できます。この場合、ユーザは検索が再開されるまでの時間を指定します。検索が再開されると、以前に検索されていたファイルもすべて再度検索されます。予約検索の停止と再開は一度だけ実行できます。

注意

ユーザが指定可能な最小延期時間は、15 分です。最大は 12 時間 45 分です。

延期時間を変更するには、[エージェント] > [グローバルエージェント設定] の [セキュリティ設定] タブに移動します。[予約検索設定] セクションで、[予約検索を最長__時間__分延期する] 設定を変更します。

予約検索のスキップおよび停止

この権限を持つユーザは次の操作を実行できます。

- 予約検索が実行される前にそれをスキップできます。
- 予約検索の実行中にそれを停止できます。

注意

予約検索を複数回スキップまたは停止することはできません。システムの再起動後も、次回の予約時刻に基づいて予約検索が再開されます。

予約検索権限の通知

ユーザが予約検索権限を利用できるようにするには、予約検索が実行される前に通知メッセージを表示するように Apex One を設定して、ユーザに付与した権限について通知します。

予約検索権限の付与と権限の通知の表示

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [権限] タブの [予約検索] セクションに移動します。
5. 次のオプションを選択します。
   - 予約検索の延期
   - 予約検索のスキップおよび停止
6. [その他の設定] タブをクリックし、[予約検索設定] セクションに移動します。
7. [予約検索の実行前に通知を表示します] を選択します。

   このオプションを有効にすると、予約検索実行の指定時間 (分単位) 前に、エージェントエンドポイントに通知メッセージが表示されます。ユーザには、検索のスケジュール (日時) および予約検索権限 (予約検索の延期、スキップ、停止など) が通知されます。

   注意

   メッセージを表示する時間を設定できます (分単位)。この時間を設定するには、[エージェント] > [グローバルエージェント設定] の [セキュリティ設定] タブに移動します。[予約検索設定] セクションで、[予約検索の実行__分前にユーザに知らせる] 設定を変更します。
8. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。
   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェン

トに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。

- 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

エージェントでの予約検索の延期/スキップおよび停止

手順

- 予約検索が起動していない場合、次の処理を実行します。

  a. タスクトレイの セキュリティエージェントアイコンを右クリックして、[予約検索の詳細設定] を選択します。

  注意

  通知メッセージが有効であり、予約検索が実行されるまでの時間が表示されるよう設定されている場合、ユーザはこの手順を実行する必要はありません。通知メッセージの詳細については、331 ページの「予約検索権限の通知」を参照してください。

  b. 表示される通知ウィンドウ上で、次のいずれかのオプションを選択します。

  - 予約検索を__時間__分延期します。
  - 予約検索をスキップします(次回の予約検索は<日付><時刻>に実行されます)。

- 予約検索が実行されている場合、次の処理を実行します。

  a. タスクトレイの セキュリティエージェントアイコンを右クリックして、[予約検索の詳細設定] を選択します。

  b. 表示される通知ウィンドウ上で、次のいずれかのオプションを選択します。

- 検索を停止し、__時間__分後に再開します。
- 検索を停止し、(次回の予約検索は<日付><時刻>に実行されます)。

メール検索権限とその他の設定

セキュリティエージェントにメール検索権限がある場合、セキュリティエージェントコンソールに [メール検索] オプションが表示されます。[メール検索] オプションには、POP3 メール検索が表示されます。

次の表は、POP3 メール検索プログラムについて説明しています。

表 7-18. メール検索プログラム

詳細	説明
目的	POP3 メールメッセージでウイルス/不正プログラムを検索します。
前提条件	• ユーザが使用するためには、管理者が Web コンソールで有効にする必要があります。 注意 POP3 メール検索を有効にするには、335 ページの「メール検索権限の付与と POP3 メール検索の有効化」を参照してください。 • ウイルス/不正プログラムに対する処理は、セキュリティエージェントコンソールから設定可能ですが、Web コンソールからは設定できません。
サポートされている検索の種類	リアルタイム検索 メールメッセージが POP3 メールサーバから取得されたときに検索が実行されます。

詳細	説明
検索結果	• 検索の完了後に参照できる、検出されたセキュリティリスクに関する情報 • 検索結果はセキュリティエージェントコンソールの [ログ] 画面に表示されない • 検索結果はサーバに送信されない
その他の詳細情報	Web レピュテーション機能を共有します。

メール検索権限の付与と POP3 メール検索の有効化

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [権限] タブの [メール検索] セクションに移動します。
5. [セキュリティエージェントコンソールにメール検索設定を表示] を選択します。
6. [その他の設定] タブをクリックし、[POP3 メール検索設定] セクションに移動します。
7. [POP3 メール検索] を選択します。
8. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。
   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。

- 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

検索用のキャッシュ設定

セキュリティエージェントでは、検索パフォーマンスを向上するために、デジタル署名や手動検索のキャッシュファイルを作成できます。手動検索の実行時、セキュリティエージェントでは最初にデジタル署名キャッシュファイルが確認され、次に検索から除外するファイルについて手動検索キャッシュファイルが確認されます。検索で多数のファイルが除外されている場合、検索時間は短くなります。

デジタル署名のキャッシュ

デジタル署名キャッシュファイルは、手動検索、予約検索、および ScanNow の実行時に使用されます。エージェントでは、ファイルの署名がデジタル署名キャッシュファイルに追加されている場合、そのファイルは検索されません。

セキュリティエージェントでは、挙動監視に使用される同じデジタル署名パターンファイルを使用して、デジタル署名キャッシュファイルが作成されます。デジタル署名パターンファイルには、トレンドマイクロが信頼できると見なした、検索から除外可能なファイルのリストが含まれています。

注意

Windows Server プラットフォームでは挙動監視は自動的に無効となります。デジタル署名キャッシュを有効にした場合、これらのプラットフォームにインストールされているセキュリティエージェントでは、キャッシュで使用するデジタル署名パターンファイルがダウンロードされ、その他の挙動監視コンポーネントはダウンロードされません。

エージェントでは、スケジュールに従ってデジタル署名キャッシュファイルが作成されます。このファイルは Web コンソールから設定できます。エージェントでは、次の目的でキャッシュが作成されます。

- 最後にキャッシュファイルが作成されてからシステムに導入された、新しいファイルの署名を追加します。
- 変更されたファイルやシステムから削除されたファイルの署名を削除します。

エージェントでは、キャッシュの作成プロセスの間、次のフォルダで信頼できるファイルが確認され、これらのファイルの署名がデジタル署名キャッシュファイルに追加されます。

- %PROGRAMFILES%
- %WINDIR%

キャッシュの作成プロセスは、最小限のシステムリソースしか使用しないため、エンドポイントのパフォーマンスに影響しません。エージェントでは、何らかの理由 (ホストコンピュータの電源が切断された場合や、ワイヤレスエンドポイントの AC アダプタのプラグが抜かれた場合など) で中断されたキャッシュの作成タスクを再開することもできます。

手動検索のキャッシュ

手動検索キャッシュファイルは、手動検索、予約検索、および ScanNow の実行時に使用されます。セキュリティエージェントでは、ファイルのキャッシュが手動検索キャッシュファイルに追加されている場合、そのファイルは検索されません。

検索を実行するたびに、セキュリティエージェントでは、脅威を含まないファイルのプロパティが確認されます。脅威を含まないファイルが特定の期間変更されていない場合 (この期間は変更可能)、セキュリティエージェントでは、このファイルのキャッシュが手動検索キャッシュファイルに追加されます。次の検索の実行時、キャッシュが期限切れになっていなければ、そのファイルは検索されません。

脅威を含まないファイルのキャッシュは、設定された期間を経過すると期限切れになります (この期間も設定可能です)。キャッシュの期限切れ以降に検索が発生した場合、セキュリティエージェントでは、期限切れキャッシュが削除され、ファイルが脅威について検索されます。ファイルが脅威を含まないファイルで、変更されないままの場合、そのファイルのキャッシュがオンデマンドの検索キャッシュファイルに再度追加されます。ファイルが脅威を

含まないファイルで、最近変更されている場合、そのファイルのキャッシュは追加されず、そのファイルは次回の検索で再度検索されます。

脅威を含まないファイルのキャッシュは、感染したファイルが検索から除外されないように、期限が定められています。

- 極端に古いパターンファイルは、感染している未変更のファイルを、脅威を含まないファイルとして処理する場合があります。キャッシュが期限切れにならなければ、この感染ファイルは、変更されてリアルタイム検索で検出されるまでシステム内に残されます。
- キャッシュのファイルが変更され、リアルタイム検索がファイルの変更時に機能しない場合は、キャッシュを期限切れにして、変更されたファイルに対して脅威を検索する必要があります。

手動検索キャッシュファイルに追加されるキャッシュの数は、検索の種類や検索対象によって変わります。たとえば、手動検索でエンドポイント内の 1,000 ファイルのうち 200 ファイルしか検索されなければ、キャッシュの数は少なくなります。

手動検索を頻繁に実行する場合は、手動検索キャッシュファイルによって検索時間が大幅に削減されます。すべてのキャッシュが期限切れでない検索タスクでは、通常 12 分かかる検索が 1 分に削減される場合もあります。ファイルが変更されない日数を減らすことと、キャッシュの期限を延ばすことは、多くの場合パフォーマンスを向上させます。比較的短い時間はファイルは変更されないため、多くのキャッシュがキャッシュファイルに追加される可能性があります。また、キャッシュの期限を長くすることは、より多くのファイルが検索でスキップされることを意味します。

手動検索をほとんど実行しない場合は、次の検索の実行時にキャッシュが期限切れになっている可能性があるため、手動検索キャッシュを無効にすることができます。

検索用のキャッシュ設定

手順

1. [エージェント] > [エージェント管理] に移動します。

2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [その他の設定] タブをクリックし、[検索用のキャッシュ設定] セクションに移動します。
5. デジタル署名キャッシュを設定します。
   a. [デジタル署名キャッシュを有効にする] を選択します。
   b. [__日ごとにキャッシュを作成します。] に、エージェントでキャッシュを作成する頻度を指定します。
6. 手動検索キャッシュを設定します。
   a. [手動検索のキャッシュを有効にする] を選択します。
   b. [__日間変更されていない安全なファイルのキャッシュを追加します。] に、ファイルのキャッシュを作成するまでに、ファイルが変更されずに維持されている必要がある日数を指定します。
   c. [安全な各ファイルのキャッシュは、__日で有効期限が切れます。] に、キャッシュファイルにキャッシュを残しておく最大日数を指定します。

   注意

   検索時に追加されたすべてのキャッシュが同じ日に期限切れになるのを防ぐために、キャッシュは、指定した最大日数の範囲内でランダムに期限切れになります。たとえば、今日 500 キャッシュをキャッシュに追加し、最大日数が 10 に指定されている場合、一部のキャッシュが翌日期限切れとなり、大部分は翌々日以降に期限切れとなります。10 日目には、残りのキャッシュがすべて期限切れになります。
7. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。
   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェン

トに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。

- 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

信頼済みプログラムリスト権限

アプリケーションコントロール、挙動監視、情報漏えい対策、デバイスコントロール、Endpoint Sensor、およびリアルタイム検索で信頼済みプロセスの検索を省略するように Apex One を設定する権限をエンドユーザに付与することができます。信頼済みプログラムリストにプログラムを追加すると、そのプログラムとそのプログラムによって開始されたプロセスはリアルタイム検索の対象から除外されます。信頼するプログラムをリストに追加すると、エンドポイントの検索パフォーマンスが向上します。

信頼済みプログラムリストの設定の付与

手順

1. [エージェント] > [エージェント管理]に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [権限] タブの [信頼済みプログラムリスト] セクションに移動します。
5. [セキュリティエージェントコンソールに信頼済みプログラムリストを表示] を選択します。
6. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。

- すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
- 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

グローバル検索設定

エージェントにグローバル検索設定を適用する方法はいくつかあります。

- 特定の検索設定を、サーバが管理するすべてのエージェントに適用したり、特定の検索権限を持つエージェントにのみ適用することができます。たとえば、予約検索の延期期間を設定した場合、予約検索の延期権限を持つエージェントのみがこの設定を使用します。
- 特定の検索設定を、すべての検索の種類に適用したり、特定の検索の種類にのみ適用することができます。たとえば、Apex One サーバおよびセキュリティエージェントの両方がインストールされているエンドポイントでは、検索から Apex One サーバデータベースを除外することができます。ただし、この設定は、リアルタイム検索の場合にのみ適用されます。
- 特定の検索設定を、ウイルス/不正プログラムまたはスパイウェア/グレーウェア (あるいはその両方) を検索するときに適用できます。

グローバル検索設定

手順

1. [エージェント] > [グローバルエージェント設定]に移動します。
2. [セキュリティ設定] タブをクリックし、各セクションでグローバル検索を設定します。

- 343 ページの「検索設定セクション」
- 349 ページの「予約検索設定セクション」

3. [システム] タブをクリックします。
4. [ソフトウェア安全性評価サービスの設定] で、[挙動監視、ファイアウォール、ウイルス対策検索に対してソフトウェア安全性評価サービスを有効にする] を設定します。

   ソフトウェア安全性評価サービスでは、不正プログラム挙動ブロック、イベント監視、ファイアウォール、またはウイルス対策検索で検出されたプログラムに関するクエリがトレンドマイクロのデータセンターに送信され、プログラムの安全性が確認されます。ソフトウェア安全性評価サービスを有効にすることによって、誤検出の確率を低くすることができます。

   注意

   ソフトウェア安全性評価サービスを有効にする前に、セキュリティエージェントのプロキシ設定 (詳細については、687 ページの「セキュリティエージェントプロキシ設定」を参照) が正しく行われていることを確認してください。プロキシ設定の誤りやインターネット接続の中断は、トレンドマイクロのデータセンターから送信される応答の延期や不達の原因となり、監視対象のプログラムが応答していないように見えます。

   また、IPv6 セキュリティエージェントでは、トレンドマイクロのデータセンターに直接クエリを送信することはできません。このようなセキュリティエージェントがトレンドマイクロのデータセンターに接続できるようにするには、IP アドレスを変換可能な DeleGate などのデュアルスタックプロキシサーバが必要です。

5. [ネットワーク] タブをクリックします。
6. [ウイルス/不正プログラムログ帯域幅設定] で、[1 時間以内に同じウイルス/不正プログラムが繰り返し検出された場合、セキュリティエージェントにより生成されるウイルス/不正プログラムログを 1 件にする] を設定します。

   Apex One で、短時間に同じウイルス/不正プログラムによる感染が複数検出された場合、ウイルスログエントリを統合します。1 つのウイルス/不正プログラムが複数回検出された場合、すぐにウイルス/不正プログラム

のログがいっぱいになり、セキュリティエージェントがログ情報をサーバに送信するときにネットワーク帯域幅が消費されます。この機能を有効にすると、作成されるウイルス/不正プログラムのログエントリ数、およびセキュリティエージェントがウイルスログ情報をサーバに送信する際に消費されるネットワーク帯域幅のを軽減できます。

7. [エージェント制御] タブをクリックします。

8. [一般設定] で、[手動検索をエンドポイントのショートカットメニューに追加] を設定します。

   この設定を有効にすると、サーバの管理対象となるすべてのセキュリティエージェントで、Windows エクスプローラで右クリックして表示されるコンテキストメニューに [Apex One での検索] オプションが追加されます。ユーザが Windows デスクトップまたは Windows エクスプローラでファイルまたはフォルダを右クリックして、このオプションを選択すると、手動検索によりファイルまたはフォルダのウイルス/不正プログラムおよびスパイウェア/グレーウェアが検索されます。

9. [保存] をクリックします。

検索設定セクション

[グローバルエージェント設定] 画面の [セキュリティ設定] タブにある [検索設定] セクションでは、次の設定を行うことができます。

Apex One サーバのデータベースフォルダをリアルタイム検索の対象から除外する

セキュリティエージェントと Apex One サーバが同じエンドポイント上に存在する場合、セキュリティエージェントではリアルタイム検索時に、サーバデータベースのウイルス/不正プログラムおよびスパイウェア/グレーウェアの検索は行われません。

ヒント

検索時のデータベースの破損を防ぐには、この設定を有効にします。

Microsoft Exchange サーバのフォルダとファイルを検索の対象から除外

セキュリティエージェントと Microsoft Exchange 2000/2003 サーバが同じエンドポイント上に存在する場合、Apex One では、手動検索、リアルタイム検索、予約検索、および ScanNow の実行時に、次の Microsoft Exchange のフォルダとファイルに対してウイルス/不正プログラムおよびスパイウェア/グレーウェアの検索を行いません。

- `¥Exchsrvr¥Mailroot¥vsi 1` にある次のフォルダ: `Queue`、`PickUp`、`BadMail`
- `.¥Exchsrvr¥mdbdata`、次のファイルを含む: `priv1.stm`、`priv1.edb`、`pub1.stm`、および `pub1.edb`
- `.¥Exchsrvr¥Storage Group`

Microsoft Exchange 2007 以降のフォルダを使用している場合は、検索除外リストに手動でフォルダを追加する必要があります。検索除外リストの詳細については、次の Web サイトを参照してください。

http://technet.microsoft.com/ja-jp/library/bb332342.aspx

検索除外リストの設定方法の詳細については、302 ページの「検索除外」を参照してください。

ファイル操作で延期検索を有効にする

管理者は、ファイルの検索に対して延期検索をするように Apex One を設定することができます。Apex One では、ユーザがファイルをコピーする際の検索処理のタイミングを延期させることにより、ファイルのコピー処理を優先させファイルコピー時のパフォーマンスを向上させることができます。

注意

延期検索には、ウイルス検索エンジン (VSAPI) のバージョン 9.713 以降が必要です。サーバのバージョンアップの詳細については、229 ページの「Apex One サーバの手動アップデート」を参照してください。

エンドポイントに対する ELAM 機能による保護を有効にする

Apex One は、エンドポイントを起動時に保護するためのセキュアブートの一部として、ELAM (Early Launch Anti-Malware) 機能をサポートしています。管理者はこの機能を有効することにより、エンドポイントの起動時に、他のサードパーティ製ソフトウェアドライバよりも先に Apex One エージェントを起動することができます。この機能によって、Apex One エージェントは OS の起動プロセス中に不正プログラムを検出できます。

すべてのサードパーティ製ソフトウェアドライバを検索した後、Apex One エージェントは、システムカーネルにドライバの分類情報を報告します。管理者は、Windows のグループポリシーのドライバ分類に基づいて処理を定義でき、エンドポイントのイベントビューアを使用して処理結果を確認できます。

注意

ELAM は、Windows 8.1 (以降)、Windows Server 2012 (以降) のプラットフォームでのみサポートされています。

圧縮ファイルの検索制限

サーバの管理対象となるすべてのセキュリティエージェントは、手動検索、リアルタイム検索、予約検索、および ScanNow の実行時に、圧縮ファイルのウイルス/不正プログラムおよびスパイウェア/グレーウェアを検索する際、次の設定をチェックします。

- 圧縮ファイルの検索制限:圧縮ファイルの処理を有効にする場合は、このオプションを選択します。
- リアルタイム検索およびその他の検索 (手動検索、予約検索、ScanNow) について、個別に次の設定を指定します。
  - 解凍後のサイズが__MB を超える場合は検索しない:Apex One は制限を上回るサイズのファイルは検索しません。
  - 圧縮ファイルでは最初の__ファイルのみを検索:Apex One は、圧縮ファイルの展開後、指定された数のファイルを検索し、残ったファイルがある場合は無視します。

圧縮ファイル内の感染ファイルのウイルス駆除/削除

サーバの管理対象となるすべてのエージェントは、手動検索、リアルタイム検索、予約検索、および ScanNow の実行時に、圧縮ファイル内のウイルス/不正プログラムを検出して、次の条件に適合すると、感染ファイルを駆除または削除します。

- Apex One で実行するように設定されている処理が「駆除」または「削除」である。感染ファイルに Apex One が実行する処理は、[エージェント] > [エージェント管理] > [設定] > [検索設定] > {検索の種類} > [処理] タブで確認できます。
- [圧縮ファイル内の感染ファイルのウイルス駆除/削除] 設定を有効にしている。この設定を有効にすると、検索時にエンドポイントのリソースの使用量が増加し、検索の実行に時間がかかる場合があります。これは、Apex One が圧縮ファイルを解凍して、圧縮ファイル内の感染ファイルを駆除/削除してから、再度そのファイルを圧縮する必要があるためです。
- 圧縮ファイル形式がサポートされている。Apex One では、ZIP や、ZIP 圧縮技術を使用する Office Open XML など、特定の圧縮ファイル形式のみがサポートされています。Excel、PowerPoint、Word などの Microsoft Office 2007 アプリケーションでは、Office Open XML が初期設定の形式として使用されます。

> **注意**
>
> サポートされる圧縮ファイル形式の全リストについては、サポート担当者にお問い合わせください。

たとえば、リアルタイム検索で、ウイルスに感染したファイルは削除するよう設定されているとします。リアルタイム検索で「`abc.zip`」という圧縮ファイルを解凍し、その中の「`123.doc`」というファイルで感染を検出した場合、Apex One は「`123.doc`」ファイルを削除し、再び「`abc.zip`」として圧縮します。再圧縮された「`abc.zip`」ファイルは安全にアクセスできるようになります。

次の表は、上記のいずれかの条件が成立しない場合に実行される処理を示しています。

表 7-19. 圧縮ファイルのシナリオと結果

[圧縮ファイル内の感染ファイルのウイルス駆除/削除]のステータス	APEX ONE で実行するように設定された処理	圧縮ファイル形式	結果
有効	駆除または削除	サポートなし 例:「def.rar」に感染ファイル「123.doc」が含まれている場合。	Apex One は「def.rar」を暗号化しますが、「123.doc」に対して駆除、削除、またはその他の処理を行いません。
無効	駆除または削除	サポートあり/サポートなし 例:「abc.zip」に感染ファイル「123.doc」が含まれている場合。	Apex One は「abc.zip」および「123.doc」に対して、駆除、削除、またはその他の処理を行いません。

[圧縮ファイル内の感染ファイルのウイルス駆除/削除] のステータス	Apex One で実行するように設定された処理	圧縮ファイル形式	結果
有効/無効	駆除や削除は実行されません。つまり、拡張子変更、隔離、アクセス拒否、または放置 (ログのみ) のいずれかになります。	サポートあり/サポートなし 例:「abc.zip」に感染ファイル「123.doc」が含まれている場合。	Apex One は「abc.zip」に対して設定された処理 (拡張子変更、隔離、アクセス拒否、または放置 (ログのみ)) を実行しますが、「123.doc」に対しては実行しません。 各設定によって、次の処理を実行します。 拡張子変更: Apex One は「abc.zip」の名前を「abc.vir」に変更します。「123.doc」の名前は変更しません。 隔離: Apex One は「abc.zip」を隔離します (「123.doc」と他のすべての未感染ファイルも隔離します)。 放置 (ログのみ): Apex One は「abc.zip」および「123.doc」に対して処理を実行せず、ウイルスが検出されたことをログに記録します。 アクセス拒否: Apex One は、「abc.zip」を開くときにアクセスを拒否します (「123.doc」と他のすべての未感染ファイルも開くことはできません)。

Cookie を検索する

Cookie が潜在的なセキュリティリスクと考えられる場合、このオプションを選択します。これを選択すると、サーバの管理対象となるすべてのエージェントは、手動検索、予約検索、リアルタイム検索、および ScanNow の実行時に、Cookie のスパイウェア/グレーウェアを検索します。

予約検索設定セクション

予約検索を実行するよう設定されたエージェントのみが、次の設定を使用します。予約検索では、ウイルス/不正プログラムおよびスパイウェア/グレーウェアを検索できます。

グローバル検索設定の予約検索設定セクションでは、次の設定を行うことができます。

予約検索の実行__分前にユーザに知らせる

Apex One は、検索実行の指定時間 (分単位) 前に、ユーザに、検索スケジュール (日時) とユーザに付与した予約検索権限を示す通知メッセージを表示します。

通知メッセージは、[エージェント] > [エージェント管理] > [設定] > [権限とその他の設定] > [その他の設定] (タブ) > [予約検索設定] から有効または無効にできます。これを無効にすると、この通知メッセージは表示されません。

予約検索を最長__時間__分延期する

「予約検索の延期」権限を持つユーザのみが、次の処理を実行できます。

- 予約検索を実行する前にそれを延期させて、その延期期間を指定できます。
- 予約検索が実行されている場合、ユーザは検索を停止して後で再開できます。この場合、ユーザは検索が再開されるまでの時間を指定します。検索が再開されると、以前に検索されていたファイルもすべて再度検索されます。

  ユーザが指定可能な最大延期時間は 12 時間 45 分です。これを短縮するには、所定のフィールドに時間と分数を指定します。

検索を__時間__分を超えて実行し続けた場合、予約検索を自動的に停止します

Apex One は、指定された時間が経過しても検索が終了しない場合、検索を停止します。検索時に検出されたセキュリティリスクは、すべてユーザにただちに通知されます。

ワイヤレスエンドポイントのバッテリ残量が__%未満で、かつ AC アダプタが接続されていない場合には、予約検索をスキップします

Apex One は、ワイヤレスエンドポイントが電源につながっておらず、バッテリが残り少ないことを検出した場合、予約検索が起動したときに検索をただちにスキップします。バッテリの残りが少なくても電源につながっていれば、検索は行われます。

実行されなかった予約検索を開始する

指定日時に Apex One が実行されていなかったために予約検索が起動しなかった場合や予約検索が中断された場合 (検索の開始後にエンドポイントの電源を切った場合など) 、検索再開時刻を指定できます。

再開する予約検索を指定します。

- 中断された予約検索の再開: エンドポイントの電源を切ったために中断された予約検索を再開します。
- 実行されなかった予約検索の再開: エンドポイントが実行されていなかったために実行されなかった予約検索を再開します。

検索をいつ再開するかを指定します。

- 翌日の同じ時刻:翌日の同一時刻に Apex One が実行されていれば、その時刻に検索を再開します。
- __分後 (エンドポイントの起動後):ユーザがエンドポイントの電源を入れてから所定の時間 (分) 後に検索を再開します。この時間は 10～120 分の範囲で指定します。

注意

管理者が予約検索の権限を有効にした場合、ユーザは予約検索の再開を延期またはスキップできます。詳細については、330 ページの「予約検索権限とその他の設定」を参照してください。

セキュリティリスク通知

Apex One には、検出されたセキュリティリスクに関する情報を、管理者、他の Apex One 管理者、およびセキュリティエージェントユーザに通知する初期設定のメッセージが用意されています。

管理者に送信される通知の詳細については、351 ページの「管理者向けのセキュリティリスクの通知」を参照してください。

セキュリティエージェントユーザに送信される通知の詳細については、358 ページの「セキュリティエージェントユーザ向けのセキュリティリスクの通知」を参照してください。

管理者向けのセキュリティリスクの通知

セキュリティリスクを検知するか、セキュリティリスクに対する処理が失敗し、介在を必要とする場合に Apex One 管理者に通知メッセージを送信するよう Apex One を設定します。

Apex One には、Apex One 管理者にセキュリティリスクの検出について通知する初期設定の通知メッセージが用意されています。これらの通知は、要件に合わせて変更したり、追加の通知を設定できます。

表 7-20. セキュリティリスクの通知の種類

種類	参照
ウイルス/不正プログラム	352 ページの「管理者向けのセキュリティリスクの通知の設定」
スパイウェア/グレーウェア	352 ページの「管理者向けのセキュリティリスクの通知の設定」

種類	参照
デジタル資産の転送	502 ページの「管理者向けの情報漏えい対策通知の設定」
C&C コールバック	526 ページの「管理者向けの C&C コールバック通知の設定」

注意

Apex One は、メール、SNMP トラップ、および Windows NT イベントログで通知を送信できます。Apex One からこれらのチャネル経由で通知を送信するタイミングを設定します。詳細については、612 ページの「管理者通知設定」を参照してください。

管理者向けのセキュリティリスクの通知の設定

手順

1. [管理] > [通知] > [管理者] に移動します。

   [管理者通知] 画面が表示されます。

2. [条件] タブで次の操作を実行します。

   a. [ウイルス/不正プログラム] セクションおよび [スパイウェア/グレーウェア] セクションに移動します。

   b. Apex One でウイルス/不正プログラムおよびスパイウェア/グレーウェアが検出されたときに通知を送信するか、またはこれらのセキュリティリスクの処理が失敗した場合にのみ通知を送信するかを指定します。

3. [メール] タブで次の操作を実行します。

   a. [ウイルス/不正プログラム検出] セクションおよび [スパイウェア/グレーウェア検出] セクションに移動します。

   b. [メールによる通知を有効にする] を選択します。

   c. [エージェントツリーのドメイン権限を持つユーザに通知を送信する] を選択します。

役割ベースの管理を使用して、エージェントツリーのドメイン権限をユーザに与えられます。特定のドメインに属するセキュリティエージェントで検出が行われると、ドメイン権限を持つユーザのメールアドレスにメールが送信されます。次の表の例を参照してください。

表 7-21. エージェントツリードメインと権限

エージェントツリードメイン	ドメイン権限を持つ役割	役割を持つユーザアカウント	ユーザアカウントのメールアドレス
ドメイン A	管理者 (ビルトイン)	root	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
ドメイン B	管理者 (ビルトイン)	root	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

ドメイン A に属しているセキュリティエージェントがウイルスを検出すると、mary@xyz.com、john@xyz.com、および chris@xyz.com にメールが送信されます。

ドメイン B に属しているセキュリティエージェントがスパイウェアを検出すると、mary@xyz.com と jane@xyz.com にメールが送信されます。

注意

このオプションを有効にする場合は、ドメイン権限を持つすべてのユーザが、対応するメールアドレスを持っている必要があります。メールアドレスを持たないユーザにはメール通知は送信されません。ユーザとメールアドレスは、[管理] > [アカウント管理] > [ユーザアカウント]で設定します。

d. [次のメールアドレスに通知メッセージを送信する] を選択し、メールアドレスを入力します。

e. メール通知で使用する件名を [件名] に指定します。

f. メッセージの内容を [メッセージ] に指定します。

Apex One の [件名] と [メッセージ] では、トークンを使用できます。

表 7-22. セキュリティリスク通知のトークン変数

変数トークン	説明
ウイルス/不正プログラム検出	
%v	セキュリティ上の脅威の名前
%s	検出を含むエンドポイント
%i	エンドポイントの IP アドレス
%c	エンドポイントの MAC アドレス
%m	エンドポイントのドメイン
%p	ウイルス/不正プログラムの場所
%y	検出の日時
%e	ウイルス検索エンジンのバージョン
%r	ウイルスパターンファイルのバージョン
%a	セキュリティリスクに対して実行された処理
%n	エンドポイントにログオンしているユーザの名前
%g	セキュリティエージェントの GUID
%b	検索の種類
スパイウェア/グレーウェア検出	
%s	検出を含むエンドポイント
%i	エンドポイントの IP アドレス
%m	エンドポイントのドメイン
%y	検出の日時

変数トークン	説明
%n	エンドポイントにログオンしているユーザの名前
%T	スパイウェア/グレーウェアと検索結果
%d	スパイウェア/グレーウェア検出に関する詳細情報
%g	セキュリティエージェントの GUID
%b	検索の種類

4. [SNMP トラップ] タブで次の操作を実行します。

   a. [ウイルス/不正プログラム検出] セクションおよび [スパイウェア/グレーウェア検出] セクションに移動します。

   b. [SNMP トラップによる通知を有効にする] を選択します。

   c. 初期設定のメッセージをそのまま使用するか変更します。[メッセージ] では、次の表に示すトークン変数を使用してデータを表現できます。

表 7-23. セキュリティリスク通知のトークン変数

変数	説明
ウイルス/不正プログラム検出	
%v	セキュリティ上の脅威の名前
%s	検出を含むエンドポイント
%i	エンドポイントの IP アドレス
%c	エンドポイントの MAC アドレス
%m	エンドポイントのドメイン
%p	ウイルス/不正プログラムの場所
%y	検出の日時
%e	ウイルス検索エンジンのバージョン
%r	ウイルスパターンファイルのバージョン

変数	説明
%a	セキュリティリスクに対して実行された処理
%n	エンドポイントにログオンしているユーザの名前
%g	セキュリティエージェントの GUID
%b	検索の種類
スパイウェア/グレーウェア検出	
%s	検出を含むエンドポイント
%i	エンドポイントの IP アドレス
%m	エンドポイントのドメイン
%y	検出の日時
%n	エンドポイントにログオンしているユーザの名前
%T	スパイウェア/グレーウェアと検索結果
%v	セキュリティ上の脅威の名前
%a	セキュリティリスクに対して実行された処理
%d	スパイウェア/グレーウェア検出に関する詳細情報
%g	セキュリティエージェントの GUID

5. [Windows イベントログ] タブで次の操作を実行します。

   a. [ウイルス/不正プログラム検出] セクションおよび [スパイウェア/グレーウェア検出] セクションに移動します。

   b. [Windows イベントログによる通知を有効にする] を選択します。

   c. 初期設定のメッセージをそのまま使用するか変更します。[メッセージ] では、次の表に示すトークン変数を使用してデータを表現できます。

表 7-24. セキュリティリスク通知のトークン変数

変数	説明
ウイルス/不正プログラム検出	
%v	セキュリティ上の脅威の名前
%s	検出を含むエンドポイント
%i	エンドポイントの IP アドレス
%c	エンドポイントの MAC アドレス
%m	エンドポイントのドメイン
%p	ウイルス/不正プログラムの場所
%y	検出の日時
%e	ウイルス検索エンジンのバージョン
%r	ウイルスパターンファイルのバージョン
%a	セキュリティリスクに対して実行された処理
%n	エンドポイントにログオンしているユーザの名前
%g	セキュリティエージェントの GUID
%b	検索の種類
スパイウェア/グレーウェア検出	
%s	検出を含むエンドポイント
%i	エンドポイントの IP アドレス
%m	エンドポイントのドメイン
%y	検出の日時
%n	エンドポイントにログオンしているユーザの名前
%T	スパイウェア/グレーウェアと検索結果
%v	セキュリティ上の脅威の名前

変数	説明
%a	セキュリティリスクに対して実行された処理
%d	スパイウェア/グレーウェア検出に関する詳細情報
%g	セキュリティエージェントの GUID

6. [保存] をクリックします。

セキュリティエージェントユーザ向けのセキュリティリスクの通知

Apex One では、次の場合にセキュリティエージェントエンドポイントに通知メッセージを表示できます。

- リアルタイム検索および予約検索でウイルス/不正プログラムおよびスパイウェア/グレーウェアが検出された直後。通知メッセージを有効にして、必要に応じてメッセージの内容を修正してください。
- 感染ファイルの駆除処理を完了するためにエンドポイントの再起動が必要な場合。リアルタイム検索の場合、特定のセキュリティリスクが検索された後にメッセージが表示されます。手動検索、予約検索、および ScanNow の場合、Apex One がすべての検索対象を検索し終えた後に一度だけメッセージが表示されます。

表 7-25. セキュリティリスクのエージェント通知の種類

種類	参照
ウイルス/不正プログラム	360 ページの「セキュリティエージェントのウイルス/不正プログラム通知の設定」
スパイウェア/グレーウェア	361 ページの「スパイウェア/グレーウェア通知の設定」
ファイアウォール違反	563 ページの「ファイアウォール通知メッセージの内容の変更」
Web レピュテーション違反	525 ページの「Web からの脅威の通知の変更」

種類	参照
デバイスコントロール違反	447 ページの「デバイスコントロール通知の変更」
挙動監視ポリシー違反	427 ページの「通知メッセージの内容の変更」
デジタル資産の転送	505 ページの「エージェント向けの情報漏えい対策通知の設定」
C&C コールバック	525 ページの「Web からの脅威の通知の変更」

ユーザへのウイルス/不正プログラムおよびスパイウェア/グレーウェアの検出の通知

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [検索設定] > [リアルタイム検索設定]、または [設定] > [検索設定] > [予約検索設定] の順にクリックします。
4. [処理] タブをクリックします。
5. 次のオプションを選択します。
   - ウイルス/不正プログラムの検出時にエンドポイントに通知を表示
   - 潜在的なウイルス/不正プログラムの検出時にエンドポイントに通知を表示
6. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。
   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。

- 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

セキュリティエージェントのウイルス/不正プログラム通知の設定

ウイルス/不正プログラムの駆除または隔離を試行した結果をエンドユーザに通知するようにセキュリティエージェントを設定できます。

手順

1. [管理] > [通知] > [エージェント]に移動します。
2. [種類] のドロップダウンから、[ウイルス/不正プログラム] を選択します。
3. 検出設定を指定します。
   a. ウイルス/不正プログラム関連のすべてのイベントに対して 1 つの通知を表示するか、次の重大度に応じて個別の通知を表示するかを選択します。
      - 高: セキュリティエージェントで処理できなかった重大な不正プログラム
      - 中: セキュリティエージェントで処理できなかった不正プログラム
      - 低: セキュリティエージェントで解決できたすべての脅威
   b. 初期設定のメッセージをそのまま使用するか変更します。
4. [保存]をクリックします。

スパイウェア/グレーウェア通知の設定

手順

1. [管理] > [通知] > [エージェント] に移動します。
2. [種類] のドロップダウンから、[スパイウェア/グレーウェア] を選択します。
3. 初期設定のメッセージをそのまま使用するか変更します。
4. [保存] をクリックします。

エージェントへの、感染ファイルの駆除処理を完了するための再起動の通知

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [その他の設定] タブをクリックし、[再起動の通知] セクションに移動します。
5. [感染ファイルの駆除処理を完了するためにエンドポイントの再起動が必要な場合に通知を表示] を選択します。
6. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。
   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。

- 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

セキュリティリスクログ

Apex One では、ウイルス/不正プログラムまたはスパイウェア/グレーウェアの検出時と、スパイウェア/グレーウェアの復元時にログが生成されます。

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログの削除スケジュールを設定します。ログの管理方法の詳細については、616 ページの「ログ管理」を参照してください。

ウイルス/不正プログラムログの表示

セキュリティエージェントは、ウイルス/不正プログラムの検出時にログを生成し、サーバにログを送信します。

手順

1. 次のいずれかに移動します。
   - [ログ] > [エージェント] > [セキュリティリスク]
   - [エージェント] > [エージェント管理]
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [ウイルス/不正プログラムログ条件] 画面に移動します。
   - [セキュリティリスクログ] 画面で、[ログの表示] > [ウイルス/不正プログラムログ] の順にクリックします。

- [エージェント管理] 画面で、[ログ] > [ウイルス/不正プログラムログ] の順にクリックします。

4. ログの条件を指定して [ログを表示する] をクリックします。
5. ログが表示されます。ログには、次の情報が含まれています。

項目	説明
日時	検出された日時
エンドポイント	検出が行われたエンドポイント
セキュリティ上の脅威	セキュリティ上の脅威の名前
感染経路	脅威の感染経路
感染ファイル/オブジェクト	エンドポイント上のファイル/オブジェクトの場所
検索の種類	脅威を検出した検索
結果	実行された処理の結果 注意 検索結果の詳細については、364 ページの「ウイルス/不正プログラムの検索結果」を参照してください。
IP アドレス	送信元エンドポイントの IP アドレスとポート番号
MAC アドレス	感染エンドポイントの MAC アドレス
詳細	特定の検出についての詳しい分析を表示するためのリンク

6. ログを CSV ファイルに保存するには、[CSV 形式ですべてエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。

   CSV ファイルには、次の情報が含まれています。

   - ログ内のすべての情報

- 検出時にエンドポイントにログオンしていたユーザの名前

ウイルス/不正プログラムの検索結果

次の検索結果がウイルス/不正プログラムログに表示されます。

表 7-26. 検索結果

結果	説明
削除	• 1 次処理は「削除」で、感染ファイルが削除されました。 • 1 次処理は「駆除」ですが、駆除は失敗しました。2 次処理は「削除」で、感染ファイルが削除されました。
隔離	• 1 次処理は「隔離」で、感染ファイルが隔離されました。 • 1 次処理は「駆除」ですが、駆除は失敗しました。2 次処理は「隔離」で、感染ファイルが隔離されました。
駆除済み	感染ファイルが駆除されました。
拡張子変更	• 1 次処理は「拡張子変更」で、感染ファイルの拡張子が変更されました。 • 1 次処理は「駆除」ですが、駆除は失敗しました。2 次処理は「拡張子変更」で、感染ファイルの拡張子が変更されました。
アクセス拒否	• 1 次処理は「アクセス拒否」で、ユーザが感染ファイルを開こうとしたときに、このファイルへのアクセスが拒否されました。 • 1 次処理は「駆除」ですが、駆除は失敗しました。2 次処理は「アクセス拒否」で、ユーザが感染ファイルを開こうとしたときに、このファイルへのアクセスが拒否されました。 • リアルタイム検索時に潜在的なウイルス/不正プログラムが検出されました。 • リアルタイム検索では、検出時の処理が「駆除」(1 次処理) と「隔離」(2 次処理) の場合でも、システム領域感染型ウイルスに感染しているファイルへのアクセスが拒否される場合があります。これは、システム領域感染型ウイルスを駆除しようとすると、感染したエンドポイントのマスターブートレコード (MBR) を破損させる可能性があるためです。手動検索を実

結果	説明
	行して、Apex One でファイルの駆除または隔離をできるようにしてください。
放置	• 1 次処理は「放置」です。Apex One は、感染ファイルに何も処理を実行しませんでした。 • 1 次処理は「駆除」ですが、駆除は失敗しました。2 次処理は「放置」のため、Apex One は感染ファイルに何も処理を実行しませんでした。
セキュリティリスクの可能性があるものを放置しました	この検索結果は、手動検索、予約検索、および ScanNow の実行時に「潜在的なウイルス/不正プログラム」が検出された場合にのみ表示されます。潜在的なウイルス/不正プログラムに関する情報と、トレンドマイクロに不審ファイルを送信して分析を依頼する方法については、トレンドマイクロのオンライン脅威データベースの次のページを参照してください。 https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/malware/possible_virus
ファイルのウイルスを駆除、またはファイルを隔離できません。	「駆除」が 1 次処理です。「隔離」が 2 次処理ですが、両方の処理が失敗しました。 解決策:365 ページの「ファイルを隔離できません。/ファイルの名前を変更できません。」を参照してください。
ファイルのウイルスを駆除、またはファイルを削除できません。	「駆除」が 1 次処理です。「削除」が 2 次処理ですが、両方の処理が失敗しました。 解決策:366 ページの「ファイルを削除できません。」を参照してください。
ファイルのウイルスを駆除、またはファイルの名前を変更できません。	「駆除」が 1 次処理です。「拡張子変更」が 2 次処理ですが、両方の処理が失敗しました。 解決策:365 ページの「ファイルを隔離できません。/ファイルの名前を変更できません。」を参照してください。
ファイルを隔離できません。/ファイルの名前を変更できません。	説明 1 感染ファイルは、別のアプリケーションによりロックされているか、実行中か、または CD 上にあります。使用しているアプリケーションがファイルを解放した後、またはファイルを実行した後に、Apex One はファイルを隔離するか拡張子を変更します。 解決策

結果	説明
	感染したファイルが CD 上にある場合、ウイルスがネットワーク上の他のエンドポイントに感染する可能性があるため、CD の使用を中止することを検討してください。
	説明 2 感染ファイルがエージェントエンドポイントの [インターネット一時ファイル] フォルダにあります。Web を参照しているときに、エンドポイントにファイルがダウンロードされたため、Web ブラウザは感染ファイルをロックした可能性があります。Web ブラウザがファイルを解放すると、Apex One はファイルを隔離するか拡張子を変更します。 解決策:なし
ファイルを削除できません。	説明 1 感染ファイルが圧縮ファイル内に存在する可能性があり、[エージェント] > [グローバルエージェント設定] の [セキュリティ設定] タブで [圧縮ファイル内の感染ファイルのウイルス駆除/削除] の設定が無効になっています。 解決策 [圧縮ファイル内の感染ファイルのウイルス駆除/削除] オプションを有効にします。この設定を有効にすると、Apex One が圧縮ファイルを解凍し、圧縮ファイル内の感染ファイルを駆除/削除して、再度ファイルを圧縮します。 注意 この設定を有効にすると、検索時にエンドポイントのリソースの使用量が増加し、検索の実行に時間がかかる場合があります。
	説明 2 感染ファイルは、別のアプリケーションによりロックされているか、実行中か、または CD 上にあります。使用しているアプリケーションがファイルを解放した後、またはファイルを実行した後に、Apex One はファイルを削除します。 解決策

結果	説明
	感染したファイルが CD 上にある場合、ウイルスがネットワーク上の他のエンドポイントに感染する可能性があるため、CD の使用を中止することを検討してください。
	説明 3 感染ファイルがセキュリティエージェントエンドポイントの [インターネット一時ファイル] フォルダにあります。Web を参照しているときに、エンドポイントにファイルがダウンロードされたため、Web ブラウザは感染ファイルをロックした可能性があります。Web ブラウザがファイルを解放すると、Apex One はファイルを削除します。 解決策:なし
指定された隔離フォルダに隔離ファイルを送信できません	Apex One はファイルをセキュリティエージェントエンドポイントの¥Suspect フォルダに隔離しましたが、指定された隔離ディレクトリにファイルを送信できませんでした。 解決策 ウイルス/不正プログラムを検出した検索の種類 (手動検索、リアルタイム検索、予約検索、または ScanNow) を特定し、[エージェント] > [エージェント管理] > [設定] > {検索の種類} > [処理] タブで指定されている隔離ディレクトリを確認します。 隔離ディレクトリが、Apex One サーバコンピュータ上または別の Apex One サーバコンピュータ上にある場合: 1. エージェントがサーバに接続可能であるかどうかを確認します。 2. 隔離ディレクトリの形式として URL を使用している場合: a. http://の後に指定したエンドポイント名が正しいことを確認します。 b. 感染ファイルのサイズを確認します。感染ファイルが[管理] > [設定] > [隔離フォルダ設定] で指定されている最大ファイルサイズを超えている場合、設定を調整します。また、ファイルを削除するなど、他の処理を実行することも可能です。 c. 隔離ディレクトリフォルダのサイズを確認し、[管理] > [設定] > [隔離フォルダ設定] で指定されているフォルダの容量を超えているかどうかを判断します。フォルダの

結果	説明
	容量を調整するか、手動で隔離ディレクトリ内のファイルを削除します。 3. UNC パスを使用する場合、隔離ディレクトリフォルダがグループ「Everyone」と共有され、このグループに読み取り/書き込み権限を割り当てていることを確認します。また、隔離ディレクトリフォルダが存在し、UNC パスが正しいかどうかを確認します。 隔離ディレクトリがネットワーク上の別のエンドポイントにある場合 (この状況では UNC パスのみを使用することができます): 1. セキュリティエージェントがエンドポイントに接続可能であるかどうかを確認します。 2. 隔離ディレクトリフォルダが「Everyone」グループで共有されていることと、このグループに対して読み取り/書き込み許可を割り当てていることを確認します。 3. 隔離ディレクトリフォルダが存在するかどうかを確認します。 4. UNC パスが正しいかどうかを確認します。 隔離ディレクトリがセキュリティエージェントエンドポイント上の別のディレクトリにある場合 (この状況では絶対パスのみを使用することができます) は、隔離ディレクトリフォルダが存在するかどうかを確認します。
ファイルのウイルスを駆除できません。	説明 1 感染ファイルが圧縮ファイル内に存在する可能性があり、[エージェント] > [グローバルエージェント設定] の [セキュリティ設定] タブで [圧縮ファイル内の感染ファイルのウイルス駆除/削除] の設定が無効になっています。 解決策 [圧縮ファイル内の感染ファイルのウイルス駆除/削除] オプションを有効にします。この設定を有効にすると、Apex One が圧縮ファイルを解凍し、圧縮ファイル内の感染ファイルを駆除/削除して、再度ファイルを圧縮します。

結果	説明
	注意 この設定を有効にすると、検索時にエンドポイントのリソースの使用量が増加し、検索の実行に時間がかかる場合があります。
	説明 2 感染ファイルがセキュリティエージェントエンドポイントの [インターネット一時ファイル] フォルダにあります。Web を参照しているときに、エンドポイントにファイルがダウンロードされたため、Web ブラウザは感染ファイルをロックした可能性があります。Web ブラウザがそのファイルを解放すると、Apex One はそのファイルを駆除します。 解決策:なし
	説明 3 このファイルのウイルスは駆除できない可能性があります。解決策と詳細については、838 ページの「ウイルス駆除できないファイル」を参照してください。
処理が必要	感染ファイルに対して設定されている処理を完了するには、ユーザの操作が必要です。[処理が必要] 列の上にマウスポインタを移動すると、次の詳細が表示されます。 • 「処理が必要です - Apex One ToolBox に含まれる脅威対策ツールキット「クリーンブート」ツールを使用してこの脅威を取り除く方法について、テクニカルサポートにお問い合わせください。」 • 「処理が必要です - Apex One ToolBox に含まれる脅威対策ツールキット「緊急起動ディスク」ツールを使用してこの脅威を取り除く方法について、テクニカルサポートにお問い合わせください。」 • 「処理が必要です - Apex One ToolBox に含まれる脅威対策ツールキット「ルートキットバスター」ツールを使用してこの脅威を取り除く方法について、テクニカルサポートにお問い合わせください。」 • 「処理が必要です - Apex One は、感染したエージェントで脅威を検出しました。エンドポイントを再起動し、セキュリティ上の脅威の駆除を完了してください。」

結果	説明
	• 「処理が必要です - 検出されたルートキットをエンドポイントから取り除くには、完全なシステムスキャンを実行する必要があります。」

隔離の一括復元ログの表示

不正プログラムの駆除後、セキュリティエージェントは不正プログラムのデータをバックアップします。データが無害であると考えられる場合は、オンラインエージェントにバックアップされたデータを復元するように通知します。バックアップデータが復元された不正プログラム、影響を受けるエンドポイント、および復元結果に関する情報は、ログで確認できます。

手順

1. [ログ] > [エージェント] > [隔離の一括復元] に移動します。
2. [成功]、[失敗]、[保留] の各列をチェックし、Apex One で隔離データが正常に復元されたかどうかを確認します。
3. 各列の件数リンクをクリックすると、影響を受ける各エンドポイントに関する詳細情報が表示されます。

   注意

   [失敗] と表示された復元については、[隔離の一括復元の詳細] 画面の [すべて復元] をクリックして、ファイルの復元を再試行できます。

4. ログを CSV ファイルに保存するには、[CSV 形式ですべてエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。

スパイウェア/グレーウェアログの表示

セキュリティエージェントは、スパイウェアとグレーウェアの検出時にログを生成し、サーバにログを送信します。

手順

1. 次のいずれかに移動します。
   - [ログ] > [エージェント] > [セキュリティリスク]
   - [エージェント] > [エージェント管理]
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [スパイウェア/グレーウェアログ条件] 画面に移動します。
   - [セキュリティリスクログ] 画面で、[ログの表示] > [スパイウェア/グレーウェアログ] の順にクリックします。
   - [エージェント管理] 画面で、[ログ] > [スパイウェア/グレーウェアログ] の順にクリックします。
4. ログの条件を指定して [ログを表示する] をクリックします。
5. ログが表示されます。ログには、次の情報が含まれています。

項目	説明
日時	検出された日時
エンドポイント	検出が行われたエンドポイント
スパイウェア/グレーウェア	セキュリティ上の脅威の名前
検索の種類	脅威を検出した検索
結果	実行された処理の結果 **注意** 検索結果の詳細については、372 ページの「スパイウェア/グレーウェアの検索結果」を参照してください。
IP アドレス	送信元エンドポイントの IP アドレスとポート番号

項目	説明
MAC アドレス	感染エンドポイントの MAC アドレス
詳細	特定の検出についての詳しい分析を表示するためのリンク

6. (オプション) 無害と考えられるスパイウェア/グレーウェアの検出を選択し、[承認済みリストに追加] をクリックしてプログラムを以降の検索から除外します。

7. ログを CSV ファイルに保存するには、[CSV 形式ですべてエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。

   CSV ファイルには、次の情報が含まれています。

   - ログ内のすべての情報
   - 検出時にエンドポイントにログオンしていたユーザの名前

スパイウェア/グレーウェアの検索結果

次の検索結果がスパイウェア/グレーウェアログに表示されます。

表 7-27. 第 1 レベルのスパイウェア/グレーウェアの検索結果

結果	説明
完了しました。処理は必要ありません	これは、検索処理が成功した場合の第 1 レベルの結果です。第 2 レベルの結果は、次のいずれかになります。 • 駆除済み • アクセス拒否

結果	説明
この後の処理が必要です	これは、検索処理が失敗した場合の第 1 レベルの結果です。第 2 レベルの結果は、次のメッセージのいずれかになります。 • 放置 (手動処理) • 保護されたシステムファイル内のスパイウェア/グレーウェアを削除できませんでした • スパイウェア/グレーウェアの検索は手動で停止されました。検索を完了してください • スパイウェア/グレーウェアは駆除されました。再起動する必要があります。コンピュータを再起動してください • スパイウェア/グレーウェアを駆除できません • スパイウェア/グレーウェアの検索結果を特定できません。テクニカルサポートに問い合わせてください

表 7-28. 第 2 レベルのスパイウェア/グレーウェアの検索結果

結果	説明	解決策
駆除済み	Apex One は、プロセスを終了したか、レジストリ、ファイル、Cookie、およびショートカットを削除しました。	なし
アクセス拒否	Apex One は、検出されたスパイウェア/グレーウェアコンポーネントへのアクセス (コピー、開く) を拒否しました。	なし
放置 (手動処理)	Apex One は、何も処理は実行しませんでしたが、評価用にスパイウェア/グレーウェアの検出をログに記録しました。	安全と考えられるスパイウェア/グレーウェアをスパイウェア/グレーウェアの承認済みリストに追加します。

結果	説明	解決策
保護されたシステムファイル内のスパイウェア/グレーウェアを削除できませんでした	スパイウェア検索エンジンが 1 つのフォルダを削除しようとした場合に、次の条件に該当していると、このメッセージが表示されます。 • 駆除する対象が 250MB を超えています。 • OS がフォルダのファイルを使用しています。このフォルダが通常のシステム操作に必要な可能性もあります。 • そのフォルダはルートディレクトリ (C:、F: など) です。	サポート担当者にお問い合わせください。
スパイウェア/グレーウェアの検索は手動で停止されました。検索を完了してください	検索が完了する前に、ユーザが中止しました。	手動検索を実行し、検索が終了するまで待機します。
スパイウェア/グレーウェアは駆除されました。再起動する必要があります。コンピュータを再起動してください	Apex One はスパイウェア/グレーウェアのコンポーネントを削除しましたが、タスクを完了するためにエンドポイントの再起動が必要です。	エンドポイントをすぐに再起動してください。
スパイウェア/グレーウェアを駆除できません	スパイウェア/グレーウェアが、CD-ROM またはネットワークドライブで検出されました。Apex One では、これらの場所で検出されたスパイウェア/グレーウェアを削除できません。	感染ファイルを手動で削除します。
スパイウェア/グレーウェアの検索結果を特定できません。テクニカルサポートに問い合わせてください	新しいバージョンのスパイウェア検索エンジンでは、Apex One で処理するように設定されていなかった新しい検索結果が出力されます。	新しい検索結果の判断については、テクニカルサポートに問い合わせてください。

スパイウェア/グレーウェア復元ログの表示

スパイウェア/グレーウェアの駆除後、セキュリティエージェントはスパイウェア/グレーウェアのデータをバックアップします。データが無害であると考えられる場合は、オンラインエージェントにバックアップされたデータを復元するように通知します。バックアップデータが復元されたスパイウェア/グレーウェア、影響を受けるエンドポイント、および復元結果に関する情報は、ログで確認できます。

手順

1. [ログ] > [エージェント] > [スパイウェア/グレーウェアの復元] に移動します。
2. [結果] 列で、スパイウェア/グレーウェアのデータの復元が成功しているかどうかを確認します。
3. ログを CSV ファイルに保存するには、[CSV 形式ですべてエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。

不審ファイルログの表示

セキュリティエージェントは、不審ファイルリストに登録されたファイルを検出するとログを生成してサーバに送信します。

手順

1. 次のいずれかに移動します。
   - [ログ] > [エージェント] > [セキュリティリスク]
   - [エージェント] > [エージェント管理]
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [ログ] > [不審ファイルログ] または [ログの表示] > [不審ファイルログ] をクリックします。

4. ログの条件を指定して [ログを表示する] をクリックします。
5. ログが表示されます。ログには、次の情報が含まれています。
   - 日時
   - エンドポイント
   - ドメイン
   - SHA-1 ハッシュ値
   - ファイルのパス
   - 検索の種類
   - 結果

     注意

     検索結果の詳細については、364 ページの「ウイルス/不正プログラムの検索結果」を参照してください。
   - IP アドレス

検索ログの表示

手動検索、予約検索、または ScanNow の実行時、セキュリティエージェントでは、検索情報を記録した検索ログが作成されます。検索ログは、Apex One サーバまたはセキュリティエージェントのコンソールにアクセスして確認できます。

検索ログを表示するには、Apex One サーバで、次のいずれかに移動します。

- [ログ] > [エージェント] > [セキュリティリスク] に移動し、[ログの表示] > [検索ログ] をクリックします。
- [エージェント] > [エージェント管理] に移動し、[ログ] > [検索ログ] をクリックします。

検索ログには、次の情報が含まれています。

- 開始日時
- 終了日時
- ステータス
  - 完了: 検索が正常に完了しました。
  - 中断: 完了前にユーザが検索を中止しました。
  - 予期しない停止: ユーザ、システム、または予期しないイベントの発生によって検索が中断されました。たとえば、リアルタイム検索サービスが予期せずに終了したり、ユーザがエンドポイントを強制的に再起動した可能性があります。
- 検索の種類
- 検索済み
- 検出されたウイルス/不正プログラム
- 検出されたスパイウェア/グレーウェア
- スマートスキャン
- ウイルスパターンファイル
- スパイウェア/グレーウェアパターンファイル

セキュリティリスクの大規模感染

特定の期間におけるウイルス/不正プログラム、スパイウェア/グレーウェア、および共有フォルダセッションの検出の件数が、所定のしきい値を超えると、セキュリティリスクの大規模感染が発生します。ネットワークでの大規模感染に対応し、これを阻止するには、次のようないくつかの方法があります。

- Apex One を有効にしてネットワークの不審な活動を監視する
- 重要なエージェントエンドポイントのポートとフォルダをブロックする
- 大規模感染警告メッセージをエージェントに発信する

- 感染したエンドポイントをクリーンナップする

セキュリティリスクのアウトブレークの基準と通知

大規模感染が発生するたびに、Apex One 管理者に通知メッセージを送信するよう Apex One を設定します。

表 7-29. セキュリティリスクのアウトブレーク通知の種類

種類	参照
• ウイルス/不正プログラムのアウトブレーク • スパイウェア/グレーウェアのアウトブレーク • 共有フォルダセッションアウトブレーク	379 ページの「セキュリティリスクのアウトブレークの基準と通知の設定」
ファイアウォール違反アウトブレーク	566 ページの「ファイアウォール違反アウトブレークの基準と通知の設定」
C&C コールバックアウトブレーク	531 ページの「C&C コールバックのアウトブレークの基準と通知の設定」

大規模感染を検出数と検出期間によって定義します。Apex One は、検出期間内に検出数が設定値を超えると、アウトブレークアラートを実行します。

Apex One には、Apex One 管理者に大規模感染について通知する初期設定のメッセージが用意されています。これらの通知は、必要に応じて変更したり、追加の通知を設定できます。

注意

Apex One は、メール、SNMP トラップ、および Windows NT イベントログ経由で、セキュリティリスクの大規模感染の通知を送信できます。共有フォルダセッションの大規模感染の場合、Apex One はメールで通知を送信します。Apex One からこれらのチャネル経由で通知を送信するタイミングを設定します。

詳細については、612 ページの「管理者通知設定」を参照してください。

セキュリティリスクのアウトブレークの基準と通知の設定

手順

1. [管理] > [通知] > [アウトブレーク] に移動します。
2. [条件] タブで次の操作を実行します。
   a. [ウイルス/不正プログラム] および [スパイウェア/グレーウェア] セクションに移動します。
   b. 検出の固有ソース数を指定します。
   c. セキュリティリスクごとに検出数と検出期間を指定します。

   ヒント

   この画面では初期設定値を使用することをお勧めします。

   Apex One は、24 時間以内に 101 件のウイルス/不正プログラムが検出されると通知を送信します。
3. [条件] タブで次の操作を実行します。
   a. [共有フォルダセッション] セクションに移動します。
   b. [ネットワーク上の共有フォルダセッションを監視する] を選択します。
   c. [共有フォルダセッション数] で、共有フォルダがあるエンドポイントと、共有フォルダにアクセスするエンドポイントを表示する数字のリンクをクリックします。

d. 共有フォルダセッション数と検出期間を指定します。

共有フォルダセッション数を超えると通知メッセージが送信されます。

4. [メール] タブで次の操作を実行します。

a. [ウイルス/不正プログラムアウトブレーク]、[スパイウェア/グレーウェアアウトブレーク]、および [共有フォルダセッションアウトブレーク] セクションに移動します。

b. [メールによる通知を有効にする] を選択します。

c. メールの受信者を指定します。

d. 初期設定のメールの件名およびメッセージをそのまま使用するか変更します。[件名] および [メッセージ] では、トークン変数を使用してデータを表現できます。

表 7-30. セキュリティリスクのアウトブレーク通知のトークン変数

変数	説明
ウイルス/不正プログラムの大規模感染	
%CV	検出されたウイルス/不正プログラムの総数
%CC	ウイルス/不正プログラムを含むエンドポイントの総数
スパイウェア/グレーウェアの大規模感染	
%CV	検出されたスパイウェア/グレーウェアの総数
%CC	スパイウェア/グレーウェアを含むエンドポイントの総数
共有フォルダセッションの大規模感染	
%S	共有フォルダセッションの数
%T	共有フォルダセッションを累積する期間
%M	期間 (分単位)

e. メールに含めるウイルス/不正プログラムおよびスパイウェア/グレーウェアの追加情報を選択します。エージェント/ドメイン名、セキュリティリスク名、検出日時、パスと感染ファイル、および検索結果を含めることができます。

f. 初期設定の通知メッセージをそのまま使用するか変更します。

5. [SNMP トラップ] タブで次の操作を実行します。

   a. [ウイルス/不正プログラムアウトブレーク] セクションおよび [スパイウェア/グレーウェアアウトブレーク] セクションに移動します。

   b. [SNMP トラップによる通知を有効にする] を選択します。

   c. 初期設定のメッセージをそのまま使用するか変更します。[メッセージ] では、トークン変数を使用してデータを表現できます。詳細については、380 ページの表 7-30 : セキュリティリスクのアウトブレーク通知のトークン変数を参照してください。

6. [Windows イベントログ] タブで次の操作を実行します。

   a. [ウイルス/不正プログラムアウトブレーク] セクションおよび [スパイウェア/グレーウェアアウトブレーク] セクションに移動します。

   b. [Windows イベントログによる通知を有効にする] を選択します。

   c. 初期設定のメッセージをそのまま使用するか変更します。[メッセージ] では、トークン変数を使用してデータを表現できます。詳細については、380 ページの表 7-30 : セキュリティリスクのアウトブレーク通知のトークン変数を参照してください。

7. [保存]をクリックします。

セキュリティリスクの大規模感染予防の設定

大規模感染が発生したら、大規模感染に対応し、これを阻止するために大規模感染予防策を実行します。予防設定は慎重に行う必要があります。設定が不適切なために、予期しないネットワークの問題が発生する可能性があるからです。

手順

1. [エージェント] > [大規模感染予防サービス] に移動します。

2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [大規模感染予防の開始] をクリックします。
4. 次のいずれかの大規模感染予防ポリシーを選択して、ポリシーを設定します。
   - 383 ページの「共有フォルダへのアクセスを制限/禁止」
   - 384 ページの「ポートのブロック」
   - 386 ページの「ファイルおよびフォルダへの書き込みを禁止」
   - 388 ページの「圧縮形式の実行可能ファイルへのアクセスを禁止」
   - 387 ページの「不正プロセス/ファイルに対する相互排他 (ミューテックス) 処理を作成」
5. 適用するポリシーを選択します。
6. 大規模感染予防を有効にしておく期間 (単位: 時間) を選択します。初期設定は 48 時間です。大規模感染予防の期間が終了する前に、手動でネットワーク設定を復元することができます。

   警告!

   大規模感染予防の有効期間が、無期限にならないようにしてください。特定のファイル、フォルダ、またはポートを無期限にブロックしたりアクセスを拒否したりするには、Apex One を使用するのではなく、エンドポイントとネットワークの設定を直接変更してください。
7. 初期設定のエージェント通知メッセージをそのまま使用するか変更します。

   注意

   大規模感染時に管理者に通知するように Apex One を設定するには、[管理] > [通知] > [アウトブレーク] の順に選択します。
8. [大規模感染予防の開始] をクリックします。

選択した大規模感染予防策は、新しいウィンドウに表示されます。

9. [大規模感染予防サービス] エージェントツリーに戻り、[大規模感染予防サービス] 列を確認します。

   大規模感染予防策が適用されているエンドポイントには、チェックマークが表示されます。

Apex One では、次のイベントをシステムイベントログに記録します。

- サーバイベント (大規模感染予防の開始と、大規模感染予防の有効化のエージェントへの通知)
- セキュリティエージェントイベント (大規模感染予防の有効化)

大規模感染予防ポリシー

大規模感染が発生したら、次のポリシーのいずれかを実行します。

共有フォルダへのアクセスを制限/禁止

大規模感染時は、共有フォルダを介してセキュリティリスクが拡大するのを防ぐために、ネットワーク上の共有フォルダへのアクセスを制限または拒否します。

このポリシーが有効であっても、ユーザはフォルダを共有できますが、新たに共有されたフォルダにはポリシーが適用されません。このため、大規模感染時はフォルダを共有しないようにユーザに通知するか、または新たに共有されたフォルダにポリシーを適用するために、ポリシーを再度配布してください。

手順

1. [エージェント] > [大規模感染予防サービス] に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。

3. [大規模感染予防の開始] をクリックします。
4. [共有フォルダへアクセスを禁止/制限] をクリックします。
5. 次のオプションから選択します。
   - 読み取りのみ許可: 共有フォルダへのアクセスを制限します。
   - アクセス拒否

   注意

   読み取りのみの設定は、アクセスを完全に拒否するようにすでに設定されている共有フォルダには適用できません。
6. [保存] をクリックします。

   [大規模感染予防の設定] 画面が再度表示されます。
7. [大規模感染予防の開始] をクリックします。

   選択した大規模感染予防策は、新しいウィンドウに表示されます。

ポートのブロック

大規模感染時に、ウイルス/不正プログラムがセキュリティエージェントエンドポイントにアクセスするために使用する脆弱なポートをブロックします。

警告!

大規模感染予防設定の構成を注意深く行ってください。使用中のポートをブロックすると、それらのポートを使用しているネットワークサービスが使用できなくなります。たとえば、信頼されたポートをブロックすると、Apex One は大規模感染の間はエージェントと通信できなくなります。

手順

1. [エージェント] > [大規模感染予防サービス] に移動します。

2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [大規模感染予防の開始] をクリックします。
4. [ポートのブロック] をクリックします。
5. 信頼されたポートをブロックするかどうかを選択します。
6. ブロックするポートを [ポートのブロック] 列で選択します。
   a. テーブルにポートが表示されない場合には、[追加] をクリックします。表示された画面で、ブロックするポートを選択して、[保存] をクリックします。
      - すべてのポート (ICMP を含む): 信頼されたポートを除くすべてのポートをブロックします。信頼されたポートもブロックする場合は、前の画面で [信頼されたポートをブロック] チェックボックスをオンにします。
      - 指定のポート
        - 代表的なポート: Apex One のポート番号を少なくとも 1 つ選択して、ポートのブロック設定を保存します。
        - トロイの木馬プログラムでよく使用されるポート: トロイの木馬プログラムに使用される代表的なポートをブロックします。
        - 1～65535 の任意のポート、またはポート範囲: 必要に応じて、ブロックするトラフィックの方向と、指定したポートをブロックする理由などのコメントを指定します。
        - Ping プロトコル (ICMP を拒否): ping 要求などの ICMP パケットのみをブロックする場合にクリックします。
   b. ブロック済みのポートの設定を編集するには、ポート番号をクリックします。
   c. 表示された画面で、設定を変更して、[保存] をクリックします。
   d. リストからポートを削除するには、ポート番号の横のチェックボックスをオンにして、[削除] をクリックします。

7. [保存] をクリックします。

   [大規模感染予防の設定] 画面が再度表示されます。

8. [大規模感染予防の開始] をクリックします。

   選択した大規模感染予防策は、新しいウィンドウに表示されます。

ファイルおよびフォルダへの書き込みを禁止

ウイルス/不正プログラムは、ホストエンドポイント上のファイルやフォルダを変更または削除する可能性があります。大規模感染時には、ウイルス/不正プログラムがセキュリティエージェントエンドポイント上のファイルやフォルダを変更または削除するのを防ぐように、Apex One を設定します。

警告!

Apex One は、マップされたネットワークドライブへの書き込みアクセスの禁止をサポートしていません。

手順

1. [エージェント] > [大規模感染予防サービス] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [大規模感染予防の開始] をクリックします。
4. [ファイルおよびフォルダへの書き込みを禁止] をクリックします。
5. ディレクトリパスを入力します。保護するディレクトリパスの入力が終わったら、[追加] をクリックします。

   注意

   ディレクトリのパスは、仮想パスではなく、絶対パスを入力してください。

6. 保護ディレクトリで保護するファイルを指定します。すべてのファイルを選択するか、特定のファイル拡張子に基づいてファイルを選択します。ファイル拡張子の場合、リストにない拡張子を指定するには、テキストボックスに拡張子を入力し、[追加] をクリックします。
7. 特定のファイルを保護するには、[ファイルの指定] で、完全なファイル名を入力し、[追加] をクリックします。
8. [保存] をクリックします。

   [大規模感染予防の設定] 画面が再度表示されます。
9. [大規模感染予防の開始] をクリックします。

   選択した大規模感染予防策は、新しいウィンドウに表示されます。

不正プロセス/ファイルに対する相互排他 (ミューテックス) 処理を作成

大規模感染予防サービスを設定することで、相互排他 (ミューテックス) 処理を利用するセキュリティ上の脅威がシステム全体への感染に必要とするリソースをオーバーライドし、これらの脅威を防止できます。大規模感染予防では、既知の不正プログラムに関連するファイルやプロセスに対して相互排他 (ミューテックス) の仕組みを用意し、不正プログラムによるこれらのリソースへのアクセスを阻止します。

ヒント

不正プログラムに対処するソリューションを実装するまでの間は、ミューテックスを使用することをお勧めします。大規模感染発生時に使用する正しいミューテックス名については、サポートにお問い合わせください。

注意

相互排他 (ミューテックス) 処理には不正変更防止サービスが必要で、また 32 ビットプラットフォームにのみ対応しています。

手順

1. [エージェント] > [大規模感染予防サービス] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [大規模感染予防の開始] をクリックします。
4. [不正プロセス/ファイルに対する相互排他 (ミューテックス) 処理を作成] をクリックします。
5. 表示されたテキストフィールドに、防御するミューテックス名を入力します。

   [+] ボタンと [-] ボタンを使用して、ミューテックス名をリストに追加、またはリストから削除します。

   注意

   大規模感染予防サービスは、最大 6 個のミューテックスの脅威に対する相互排他 (ミューテックス) 処理をサポートしています。

6. [保存] をクリックします。

   [大規模感染予防の設定] 画面が再度表示されます。

7. [大規模感染予防の開始] をクリックします。

   選択した大規模感染予防策は、新しいウィンドウに表示されます。

圧縮形式の実行可能ファイルへのアクセスを禁止

大規模感染時に実行可能な圧縮ファイルへのアクセスを禁止すると、これらのファイルに含まれている可能性があるセキュリティリスクがネットワーク全体に拡大するのを防ぐことができます。また、サポートされる実行可能なパッカープログラムで作成された信頼できるファイルへのアクセスを許可することもできます。

手順

1. [エージェント] > [大規模感染予防サービス] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [大規模感染予防の開始] をクリックします。
4. [圧縮形式の実行可能ファイルへのアクセスを禁止] をクリックします。
5. サポートされる実行可能なパッカープログラムのリストから選択し、[追加] をクリックして、そのパッカープログラムによって作成された実行可能なパックファイルへのアクセスを許可します。

   注意

   承認できるのは、承認済みパッカーリストにあるパッカープログラムによって作成されたパックファイルの使用だけです。大規模感染予防サービスは、その他すべての実行可能なパックファイルへのアクセスを禁止します。

6. [保存] をクリックします。

   [大規模感染予防の設定] 画面が再度表示されます。

7. [大規模感染予防の開始] をクリックします。

   選択した大規模感染予防策は、新しいウィンドウに表示されます。

大規模感染予防サービスの無効化

大規模感染が抑制され、Apex One によりすべての感染ファイルがすでに駆除または隔離されたと確信できる場合には、大規模感染予防サービスを無効にしてネットワークの設定を通常の状態に戻します。

手順

1. [エージェント] > [大規模感染予防サービス] に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定の復元] をクリックします。
4. ユーザに大規模感染が終了したことを通知するには、[初期設定の復元後にユーザに通知] を選択します。
5. 初期設定のエージェント通知メッセージをそのまま使用するか変更します。
6. [設定の復元] をクリックします。

   注意

   ネットワーク設定を手動で復元しない場合には、[大規模感染予防の設定] 画面の [自動的に大規模感染予防措置を停止する] に指定されている時間が経過した後に、Apex One により自動的にこれらの設定が復元されます。初期設定は 48 時間です。

   Apex One では、次のイベントをシステムイベントログに記録します。

   - サーバイベント (大規模感染予防の開始と、大規模感染予防の有効化のセキュリティエージェントへの通知)
   - セキュリティエージェントイベント (大規模感染予防の有効化)
7. 大規模感染予防を無効にした後、大規模感染が抑制されたことを確認するために、ネットワーク上のエンドポイントのセキュリティリスクを検索します。

第 8 章

未知の脅威からの保護

この章では、ネットワークへの侵入を試みる不明な脅威からエンドポイントを保護する方法について説明します。

この章は次のトピックで構成されます。

機械学習型検索

トレンドマイクロの機械学習型検索は、高度な機械学習テクノロジを使用して脅威情報を関連付け、デジタル DNA フィンガープリントや API マッピングなどのファイル機能を使用した詳細なファイル分析により未知のセキュリティリスクを検出します。また、不明なプロセスやあまり普及していないプロセスの挙動分析を実行して、ネットワークへの侵入を試みる未知の新しい脅威がないかどうかを判定します。

機械学習型検索は、未知の脅威およびゼロデイ攻撃から環境を保護するのに役立つ強力な検索方法です。

検出の種類	説明
ファイル	不明なファイルやあまり普及していないファイルを検出すると、セキュリティエージェントは、高度な脅威検索エンジン (ATSE) でファイルを検索してファイル特性を抽出し、Trend Micro Smart Protection Network でホストされる機械学習型検索エンジンにレポートを送信します。機械学習型検索では、不正プログラムモデリングにより、サンプルを不正プログラムモデルと比較し、可能性スコアを割り当て、ファイルに含まれる潜在的な不正プログラムの種類を判別します。 インターネット接続が使用できなくなった場合は、機械学習型検索が自動的にローカルモデルに切り替わって未知の脅威からの継続的な保護を実現し、Portable Executable ファイルの脅威に対応します。 機械学習型検索の設定に応じて、ネットワークへの脅威の拡散を防ぐために、セキュリティエージェントは該当するファイルの「隔離」を試みます。

検出の種類	説明
プロセス	不明なプロセスやあまり普及していないプロセスを検出すると、セキュリティエージェントは、CI エンジンを使用してプロセスを監視し、動作レポートを機械学習型検索エンジンに送信します。機械学習型検索では、不正プログラムの動作モデリングにより、サンプルをモデルと比較し、可能性のスコアを割り当て、プロセスが実行する潜在的な不正プログラムの種類を判別します。 プロセスの検出ではスクリプトの実行も監視対象となります。CI エンジンが不審スクリプトの実行を検出すると、機械学習型検索は設定された処理を実行します。 機械学習型検索では、次の種類のスクリプトに対してスクリプトのブロックを実行します。 • cscript • jar • powershell • vbs • wscript 機械学習型検索の設定に応じて、セキュリティエージェントは該当するプロセスまたはスクリプトを「終了」し、プロセスまたはスクリプトを実行したファイルの駆除を試みます。

機械学習型検索の設定

注意

機械学習型検索を使用するには、次のサービスを有効にする必要があります。

- 不正変更防止サービス
- 高度な保護サービス

詳細については、650 ページの「セキュリティエージェントの追加サービス設定」を参照してください。

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [機械学習型検索設定] をクリックします。

   [機械学習型検索設定] 画面が表示されます。
4. [機機械学習型検索を有効にする] を選択します。
5. [検出設定] で、機械学習型検索で実行する検出の種類とそれに対する処理を選択します。

検出の種類	処理
ファイル	• 隔離: 機械学習型検索による分析で不正プログラムに似た特性を示すと判定されたファイルを自動的に隔離する場合に選択します。 • ログのみ: 脅威について内部で詳しく調査するために、不明なファイルを検索して機械学習型検索による分析をログに記録する場合に選択します。
プロセス	• 終了: 機械学習型検索による分析で不正プログラムに似た挙動を示すと判定されたプロセスまたはスクリプトを自動的に終了する場合に選択します。  重要 機械学習型検索は、不正なプロセスまたはスクリプトを実行したファイルの駆除を試みます。駆除に失敗した場合、該当するファイルはセキュリティエージェントによって隔離されます。 • ログのみ: 脅威について内部で詳しく調査するために、不明なプロセスまたはスクリプトを検索して機械学習型検索による分析をログに記録する場合に選択します。

6. [除外] で、機械学習型検索のグローバル除外ファイルリストを設定します。このリストに追加したファイルは、いずれのエージェントでも不正ファイルとして検出されなくなります。

a. [ファイルハッシュを追加] をクリックします。

[ファイルを除外リストに追加] 画面が表示されます。

b. 検索から除外するファイルの SHA-1 ハッシュ値を指定します。

c. 必要に応じて、除外する理由やハッシュ値に関連付けられているファイル名を入力します。

d. [追加] をクリックします。

ファイルハッシュが除外リストに追加されます。

7. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。

- すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
- 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

不審接続監視サービス

不審接続監視サービスは、ユーザ指定およびグローバル IP C&C リストを管理し、エンドポイントから潜在的な C&C サーバへの接続の挙動を監視します。

- ユーザ指定の承認済みおよびブロック済み IP リストを使用すると、エンドポイントから特定の IP アドレスへのアクセスを許可するかどうかも制御できます。グローバル C&C IP リストでブロックされたアドレスへのアクセスを許可する場合や、セキュリティリスクをもたらす可能性があるアドレスへのアクセスをブロックする場合は、これらのリストを設定します。

詳細については、396 ページの「ユーザ指定の IP リストのグローバル設定」を参照してください。

- グローバル C&C IP リストは、ネットワークコンテンツ検査エンジン (NCIE) と連携して機能し、トレンドマイクロで確認済みの C&C サーバとのネットワーク接続を検出します。NCIE は、任意のネットワークチャネル経由で C&C サーバとの接続を検出します。不審接続監視サービスは、グローバル C&C IP リスト内のすべてのサーバへの接続情報をログに記録します。

  グローバル C&C IP リストの有効化については、397 ページの「不審接続監視の設定」を参照してください。

- ネットワークパケットを適合度ルールパターンファイルとの照合によってエンドポイントで不正プログラムが検出された場合、不審接続監視サービスでは、接続をさらに調査して C&C コールバックが発生したかどうかを特定できます。C&C コールバックが検出された場合、Generic Clean テクノロジを使用して接続元をブロックおよび駆除できます。

  不審接続監視サービスの設定については、397 ページの「不審接続監視の設定」を参照してください。

  Generic Clean の詳細については、827 ページの「Generic Clean」を参照してください。

C&C サーバコールバックからエージェントを保護するには、[追加サービス設定] 画面で不審接続監視サービスを有効にします。詳細については、650 ページの「セキュリティエージェントの追加サービス設定」を参照してください。

ユーザ指定の IP リストのグローバル設定

管理者は、エージェントとユーザ指定の C&C IP アドレス間のすべての接続を許可、ブロック、またはログに記録するように Apex One を設定できます。

注意

ユーザ指定の IP リストに指定できるのは、IPv4 アドレスのみです。

手順

1. [エージェント] > [グローバルエージェント設定] に移動します。
2. [セキュリティ設定] タブをクリックします。
3. [不審接続監視設定] セクションに移動します。
4. [ユーザ定義の IP リストを編集] をクリックします。
5. [承認済みリスト] タブまたは [ブロックリスト] タブで、監視する IP アドレスを追加します。

   ヒント

   ブロックリストに含まれるアドレスへの接続のみをログに記録するように Apex One を設定できます。詳細については、397 ページの「不審接続監視の設定」を参照してください。

   a. [追加] をクリックします。

   b. 表示された画面で、Apex One で監視する IP アドレス、IP アドレス範囲、または IPv4 アドレスとサブネットマスクを入力します。

   c. [保存] をクリックします。
6. リストから IP アドレスを削除するには、アドレスの横のチェックボックスをオンにして、[削除] をクリックします。
7. リストの設定後、[閉じる] をクリックして [グローバルエージェント設定] 画面に戻ります。
8. [保存] をクリックして、アップデートされたリストをエージェントに配信します。

不審接続監視の設定

セキュリティエージェントでは、エンドポイントとグローバル C&C IP リスト内のアドレス間の接続をすべてブロックしてログに記録できます。ログに記録したうえで、ユーザ指定のブロック IP リストに設定された IP アドレスへのアクセスを許可することもできます。

また、ボットネットやその他の不正プログラムに起因する接続も監視でき、不正プログラムの脅威が検出された場合はこれを駆除できます。

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [不審接続監視設定] の順にクリックします。

   [不審接続監視設定] 画面が表示されます。
4. トレンドマイクロで確認済みの C&C サーバへの接続を監視するには、[グローバル C&C IP リスト内のアドレスへのネットワーク接続を検出] 設定を有効にし、[ログのみ] または [ブロック] のいずれかを選択します。
   - ユーザ指定ブロック IP リスト内のアドレスへの接続をエージェントに許可するには、[ユーザ指定ブロック IP リスト内のアドレスへのアクセスを許可してログに記録] 設定を有効にします。

     注意

     ユーザ指定ブロック IP リスト内のアドレスへのアクセスを許可するためには、まず [グローバル C&C IP リスト内のアドレスへのネットワーク接続をログに記録] を有効にする必要があります。

   グローバル C&C IP リストの詳細については、395 ページの「不審接続監視サービス」を参照してください。
5. [不正プログラムネットワークフィンガープリントを使用して接続を検出] 設定を有効にし、[ログのみ] または [ブロック] のいずれかを選択します。

   不正プログラムネットワークフィンガープリントにより、パケットヘッダーのパターンマッチングが実行されます。セキュリティエージェントは、適合度ルールパターンファイルを使用して、ヘッダーが既知の不正プログラムに一致するパケットからの接続をすべてログに記録します。

- C&C サーバへの接続を止めるには、[C&C コールバックの検出時に不審接続監視元を駆除] 設定を有効にします。セキュリティエージェントは、GeneriClean を使用して不正プログラムの脅威を駆除し、C&C サーバへの接続を終了します。

注意

パケット構造のマッチングで検出された C&C サーバへの接続を止めるためには、まず [不正プログラムネットワークフィンガープリントを使用して接続をログに記録] を有効にする必要があります。

6. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。

   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
   - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

サンプル送信

まだ特定されていない未知の脅威を含む可能性があるファイルオブジェクトが検出された場合、詳しい分析のために仮想アナライザに送信するようにセキュリティエージェントを設定できます。オブジェクトが未知の脅威を含むと判定した場合、仮想アナライザはオブジェクトを不審オブジェクトリストに追加し、そのリストをネットワーク上の他のすべてのセキュリティエージェントに配信します。

詳細については、608 ページの「不審オブジェクトリスト設定」を参照してください。

サンプル送信を実行するための要件は次のとおりです。

- Apex One サーバを Control Manager サーバ (7.0 以降) または Trend Micro Apex Central サーバ (2019 以降) に登録する必要があります。
- Control Manager サーバまたは Trend Micro Apex Central サーバを Trend Micro Deep Discovery Analyzer サーバ (5.1 以降) に接続する必要があります。

不審ファイルには以下が含まれます。

- トレンドマイクロで認識していないプログラム (サポート対象の Web ブラウザまたはメールからダウンロード)
- ヒューリスティック検索で検出されたプロセス (サポート対象の Web ブラウザまたはメールからダウンロード)
- リムーバブルストレージ上のあまり普及していない自動実行プログラム

重要

セキュリティエージェントから送信できるサンプルファイルのサイズは、使用する仮想アナライザの種類に応じて異なります。Deep Discovery Analyzer サーバの場合、サンプルファイルの最大サイズは 50MB です。Deep Discovery Analyzer as a Service アドオンの場合、サンプルファイルの最大サイズは 60MB です。

サンプル送信の設定

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [サンプル送信設定] をクリックします。

   [サンプル送信設定] 画面が表示されます。
4. [仮想アナライザへの不審ファイルの送信を有効にする] を選択します。

5. [保存] をクリックします。

不明な脅威ログ

セキュリティエージェントでは、不明な脅威の活動がログに記録され、サーバに送信されます。継続的に実行されているセキュリティエージェントではログが集約され、指定された時間間隔で送信されます。この間隔は初期設定では 1 時間です。

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログの削除スケジュールを設定します。ログの管理方法の詳細については、616 ページの「ログ管理」を参照してください。

機械学習型検索ログの表示

手順

1. 次のいずれかに移動します。
   - [ログ] > [エージェント] > [セキュリティリスク]
   - [エージェント] > [エージェント管理]
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [機械学習型検索ログ条件] 画面に移動します。
   - [セキュリティリスクログ] 画面で、[ログの表示] > [機械学習型検索ログ] の順にクリックします。
   - [エージェント管理] 画面で、[ログ] > [機械学習型検索ログ] の順にクリックします。
4. ログの条件を指定して [ログを表示する] をクリックします。

5. ログが表示されます。ログには、次の情報が含まれています。

項目	説明
日時	検出された日時
エンドポイント	検出が行われたエンドポイント
IP アドレス	送信元エンドポイントの IP アドレスとポート番号
セキュリティ上の脅威	機械学習型検索エンジンで判定されたセキュリティ上の脅威の名前
結果	実行された処理の結果
感染ファイル/オブジェクト	ファイルオブジェクトの名前またはプロセスを実行したプログラムの名前
種類	検出を実行したオブジェクトの種類(「ファイル」または「プロセス」)
ファイルパス	ファイルオブジェクトのパスまたはプロセスを実行したプログラムのパス
感染経路	脅威の感染経路
詳細	特定の検出についての詳しい分析を表示するためのリンク 詳細については、402 ページの「機械学習型検索ログの詳細」を参照してください。

6. ログを CSV ファイルに保存するには、[CSV 形式ですべてエクスポート]をクリックします。ファイルを開くか、特定の場所に保存します。

機械学習型検索ログの詳細

[詳細] 列の [表示] リンクをクリックすると、機械学習型検索ログに検出された個々のイベントに関する詳細なレポートを表示できます。

[ログ詳細] 画面は次の 2 つのセクションで構成されます。

- 上部のバナー: このログイベントに関する情報

- 下部のタブ: 機械学習型検索の脅威に関する詳細 (脅威の可能性スコア、ファイル情報、同じ脅威が検出されたネットワーク上の他のエンドポイントなど)

次の表に、上部のバナーに表示される情報を示します。

表 8-1. ログ詳細 - 上部のバナー

セクション	説明
検出日時/処理	このログイベントの発生日時と脅威に対してエージェントが行った処理が表示されます。
ファイル名	指定したエンドポイントでイベントの検出を実行したファイルの名前が表示されます。 **ヒント** [除外リストに追加] をクリックすると、該当するファイルのファイルハッシュ値が機械学習型検索のグローバル除外リストに追加されます。除外リスト全体は [機械学習型検索の設定] 画面で確認できます。 詳細については、393 ページの「機械学習型検索の設定」を参照してください。 **重要** この検出で報告されたファイル名は、他のエージェントで検出されたファイル名と同じではない場合があります。機械学習型検索では、それぞれのファイルの名前ではなく、ファイルのハッシュ値に基づいて検出イベントを関連付けます。他のエンドポイントのファイル名を確認するには、[感染エンドポイント] タブを表示してください。
エンドポイント情報	検出時にログオンしていたユーザ、エンドポイント名、およびエンドポイントの IP アドレスが表示されます。
チャネル情報	脅威の発生元のチャネルと転送先のエンドポイントのフォルダが表示されます。

次の表に、下部のタブに表示される情報を示します。

表 8-2. ログ詳細 - タブの情報

タブ	説明
脅威の指標	機械学習型検索による分析結果が表示されます。 • 脅威の可能性: ファイル/プロセスの不正プログラムモデルに対する一致スコアを示します。 • 潜在的な脅威の種類: ファイルの内容を機械学習型検索による分析で他の既知の脅威と比較した結果、最も可能性が高いと判定された脅威の種類を示します。 • 脅威 ID: ファイル/プロセスで使用されている API 関数のうち、検出された脅威の種類に関連する API 関数のリストが表示されます。 重要 API 関数は、脅威の種類を特定するための 1 つの指標にすぎません。機械学習型検索では、他にもさまざまなファイル特性や分析方法を使用して、脅威の可能性と潜在的な脅威の種類を判定します。 • 類似する既知の脅威: 検出されたファイル/プロセスと特性が類似した既知の脅威の種類のリストが表示されます。
ファイルの詳細	この検出ログについて、ファイルプロパティおよび証明書情報に関連する一般的な詳細が表示されます。
感染エンドポイント	機械学習型検索で同じ脅威が検出されたネットワーク上の他のエージェントのリストが表示されます。他のエージェントでの検出に関する個別の情報も表示されます。

不審接続監視ログの表示

手順

1. 次のいずれかに移動します。
   - [ログ] > [エージェント] > [セキュリティリスク]
   - [エージェント] > [エージェント管理]

2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [不審接続監視ログ条件] 画面に移動します。
   - [セキュリティリスクログ] 画面で、[ログの表示] > [不審接続監視ログ] の順にクリックします。
   - [エージェント管理] 画面で、[ログ] > [不審接続監視ログ] の順にクリックします。
4. ログの条件を指定して [ログを表示する] をクリックします。
5. ログが表示されます。ログには、次の情報が含まれています。

項目	説明
日時	検出された日時
エンドポイント	検出が行われたエンドポイント
ドメイン	検出が行われたエンドポイントドメイン
プロセス	接続が試行されたプロセス (path\application_name)
ローカル IP およびポート	送信元エンドポイントの IP アドレスとポート番号
リモート IP およびポート	送信先エンドポイントの IP アドレスとポート番号
結果	実行された処理の結果
リストのソース	C&C サーバを特定した C&C リストのソース
トラフィック方向	転送の方向

6. ログを CSV ファイルに保存するには、[CSV 形式ですべてエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。

サンプル送信ログの表示

Apex One では、サンプル送信データがシステムイベントログに格納されます。サンプル送信データの概要をより詳しく確認するには、Apex Central コ

ンソールを使用してログを表示することをお勧めします。Apex Central を使用すると、不審オブジェクトファイルの処理に関する詳細な分析が提供されるため、不審オブジェクトによるネットワークへの影響を把握しやすくなります。

手順

1. [ログ] > [システムイベント] に移動します。
2. [イベント] で、次の種類のログを確認します。
   - 「サンプルが仮想アナライザに送信されました [ファイル: <ファイル名>、SHA1: <ファイルの SHA1 値>]」
   - 「仮想アナライザでのサンプルの分析が完了しました [<分析の完了日時>、ファイル: <ファイル名>、SHA1: <ファイルの SHA1 値>、ルール: <仮想アナライザのルールの種類>]」

第 9 章

挙動監視の使用

この章では、挙動監視機能を使用してセキュリティリスクからコンピュータを保護する方法について説明します。

この章は次のトピックで構成されます。

挙動監視

挙動監視機能は、エンドポイントの OS またはインストールされたソフトウェアに対して不審な変更が行われていないかどうかを常に監視します。挙動監視では、「不正プログラム挙動ブロック」と「イベント監視」によってエンドポイントが保護されます。さらにこの 2 つの機能を補うものとして、ユーザが設定する「除外リスト」と、「ソフトウェア安全性評価サービス」が使用されます。

重要

Windows Server コンピュータでは、いずれのバージョンでも初期設定で挙動監視が無効になっています。

不正プログラム挙動ブロック

不正プログラム挙動ブロックにより、不正プログラムの挙動を示すプログラムからの追加の脅威に対する保護に必要な層を提供します。不正プログラム挙動ブロックは長時間にわたり、システムイベントを観察します。プログラムが通常とは異なるシーケンスまたは組み合わせの処理を実行すると、不正プログラム挙動ブロックが既知の不正プログラムの挙動を検出して、関連プログラムをブロックします。この機能を使用すると、新たに出現した脅威に対する保護のレベルを向上できます。

挙動監視では、正規の Windows プログラムによって実行された不正なスクリプトおよび正規の DLL によって実行されたスクリプトファイルの実際のペイロードのパスを検出して、ファイルレス攻撃で隠されている不正プログラムに対してエンドポイントを保護できます。

不正プログラム挙動監視は次の脅威レベルの検索オプションを提供します。

- 既知の脅威:既知の不正プログラムの脅威に関連付けられた挙動をブロックします。
- 既知および潜在的な脅威: 既知の脅威に関連付けられた挙動をブロックし、潜在的に不正な挙動に対して処理を実行します。

通知が有効になっているプログラムをブロックした後、セキュリティエージェントはエンドポイントに通知を表示します。

通知の詳細については、425 ページの「セキュリティエージェントユーザへの挙動監視通知」を参照してください。

ランサムウェア対策

ランサムウェア対策は、「ランサムウェア」によるエージェント上のファイルの不正な変更や暗号化を防止します。ランサムウェアは不正プログラムの一種で、ファイルへのアクセスを制限し、ファイルの復元と引き換えに金銭を要求してきます。

Apex One には、ランサムウェアの脅威から環境を保護する対策として次のオプションが用意されています。

注意

セキュリティエージェントで安全なプロセスが不正プロセスとして検出される確率を少なくするには、エージェントがインターネットにアクセスし、トレンドマイクロのサーバを使用してその他の検証プロセスを実行できるようにします。

オプション	説明
不正な暗号化や変更から文書を保護	ランサムウェアの可能性のある特定のイベントシーケンスを検出するように、挙動監視を設定できます。セキュリティエージェントは、次のすべての条件に該当する場合、不正なプログラムを終了して隔離を試みます。 1. 一定期間内に 3 つのファイルを変更、削除、または名前変更しようとする、安全と認識されていないプロセス 2. 保護されているファイルの拡張子の種類を変更しようとしたプロセス さらに、[不審なプログラムによって変更されたファイルを自動的にバックアップして復元] を有効にすると、ランサムウェアによって暗号化の対象とされやすいファイルのコピーが事前にエンドポイントに作成されます。暗号化プロセスの完了後に Apex One でランサムウェアの脅威が検出されると、影響を受けたファイルの復元を求めるメッセージが表示され、事前にバックアップされていたファイルを復元する事で、データを失うリスクを低減できます。 **注意** 自動ファイルバックアップを実行するには、エージェントエンドポイントに 100MB 以上のディスク容量が必要です。また、バックアップされるのは 10MB 未満のファイルだけです。 エージェントエンドポイントのバックアップフォルダの場所は、<エージェントインストールフォルダ>¥CCSF¥module¥DRE¥data です。 **警告!** [不審なプログラムによって変更されたファイルを自動的にバックアップして復元] を有効にしないと、Apex One で新しいランサムウェアの脅威による攻撃を最初に受けたファイルを回復できません。
ランサムウェアに関連付けられていることの多いプロセスをブロック	多くのランサムウェアは、エンドポイントの特定の場所に実行可能ファイルとして侵入し、ファイルのハイジャックを試みます。該当する場所から開始されるプロセスをブロックすることで、ランサムウェアによるファイルのハイジャックを回避できます。

オプション	説明
プログラム検査を有効にして不正な実行可能ファイルを検出およびブロック	プログラム検査は、プロセスを監視して API フックを行うことで、予期しない挙動を示すプログラムを特定します。これにより、不正な実行可能ファイルの全体的な検出率が高くなりますが、システムのパフォーマンスが下がる場合があります。 **ヒント** [ブロックする脅威] リストから [既知の脅威と潜在的な脅威] を選択すると、プログラム検査によるセキュリティが向上します。

脆弱性対策

脆弱性対策は、プログラム検査と連携して機能し、プログラムの挙動を監視して、プログラムの脆弱性を悪用した攻撃の疑いがある異常な動作を検出します。不審な動作が検出されると、挙動監視によってプログラムのプロセスが終了されます。

重要

脆弱性対策を使用するには、[プログラム検査を有効にして不正な実行可能ファイルを検出およびブロック] を選択する必要があります。

新たに検出されたプログラム対策

挙動監視は Web レピュテーションサービスおよびリアルタイム検索と連携して機能し、Web チャネル、メールアプリケーション、または Microsoft Office マクロスクリプト経由でダウンロードされたファイルの普及度を確認します。「新たに検出された」ファイルが検出された後に、管理者は、ユーザがファイルを実行する前にユーザに確認を求めるように設定することができます。トレンドマイクロでは、ファイルの検出数、または Smart Protection Network により特定されたファイルの存続期間に基づいて、新たに検出されたプログラムを分類します。

挙動監視は各チャネルで次のファイルタイプを検索します。

- Web (HTTP/HTTPS): .exe ファイルを検索します。
- メールアプリケーション: .exe ファイル、および暗号化されていない.zip ファイルや.rar ファイルに含まれる圧縮された.exe ファイルを検索します。

注意

- このプロンプトが表示される前にセキュリティエージェントで HTTP/HTTPS トラフィックを検索できるようにするためには、管理者はエージェントの Web レピュテーションサービスを有効にする必要があります。
- セキュリティエージェントは、処理実行中にメールアプリケーションを介してダウンロードされたファイル名を一致させます。ファイル名が変更されると、ユーザにプロンプトは表示されません。

イベント監視

イベント監視は、不正なソフトウェアおよび不正なプログラムによる攻撃に対して保護するためのより一般的なアプローチを提供します。イベント監視では、システムエリアで特定のイベントを監視して、管理者がこのようなイベントを実行するプログラムを制御できるようにします。不正プログラム挙動ブロックで提供される保護を超える特別なシステム要件がある場合は、イベント監視を使用してください。

次の表は監視対象のシステムイベントの一覧を示しています。

表 9-1. 監視対象のシステムイベント

イベント	説明
システムファイルの複製	多くの不正プログラムは、Windows システムファイルが使用しているファイル名を使って、自分自身または他の不正プログラムのコピーを作成します。これは、通常、システムファイルの上書きまたは置換、検出の回避、またはユーザによる不正ファイルの削除を阻止する目的で実行されます。

イベント	説明
Hosts ファイルの変更	Hosts ファイルは、ドメイン名と IP アドレスを比較し、一致しているかどうかを確認します。不正プログラムの多くは、感染した Web サイト、存在しない Web サイト、または偽の Web サイトに Web ブラウザをリダイレクトするように Hosts ファイルを変更します。
不審な挙動	不審な挙動とは、正規プログラムではまれにしか実行されない特定の処理または処理グループです。不審な挙動を示すプログラムは、注意して使用する必要があります。
Internet Explorer プラグインの追加	スパイウェア/グレーウェアは、多くの場合、ツールバーやブラウザヘルパーオブジェクトを含む不要な Internet Explorer プラグインをインストールします。
Internet Explorer 設定の変更	不正プログラムは、ホームページ、信頼する Web サイト、プロキシサーバの設定、メニュー拡張などの Internet Explorer の設定を変更することがあります。
セキュリティポリシー設定の変更	Windows セキュリティポリシーを変更して、不要なアプリケーションを実行し、システム設定を変更させる場合があります。
DLL (プログラムライブラリ) インジェクション	不正プログラムの多くは、すべてのアプリケーションがプログラムライブラリ (DLL) を自動的にロードするように、Windows を設定します。これにより、アプリケーションが起動するたびに、DLL 内の不正なルーチンが実行されるようになります。
シェル設定の変更	多くの不正プログラムは、Windows シェルの設定を変更し、それらを特定のファイルタイプに関連付けます。ユーザが Windows エクスプローラで関連付けられたファイルを開くと、このルーチンによって不正プログラムが自動的に起動します。不正プログラムは、Windows シェルの設定を変更することで、使用されているプログラムの追跡を可能にしたり、正規のアプリケーションと一緒に自身を起動できるようにしたりします。
サービスの追加	Windows サービスは特殊な機能を持ち、通常はフル管理アクセス権でバックグラウンドで継続して実行されるプロセスです。不正プログラムは、自身をサービスとしてインストールし、隠れた状態のままでいることがあります。

イベント	説明
システムファイルの変更	特定の Windows システムファイルは、スタートアッププログラムやスクリーンセーバの設定を含む、システムの挙動を決定します。多くの不正プログラムは、システムファイルを変更することで、スタートアップ時に自動的に起動し、システムの挙動を制御できるようにします。
ファイアウォールポリシー設定の変更	Windows ファイアウォールポリシーは、ネットワークにアクセス可能なアプリケーション、通信用に開くポート、コンピュータと通信可能な IP アドレスを決定します。多くの不正プログラムは、このポリシーを変更して、自身がネットワークとインターネットへアクセスできるようにします。
システムプロセスの変更	多くの不正プログラムが組み込み Windows システムのプロセスでさまざまな処理を実行します。これらの処理には、実行中のプロセスを終了または変更するものがあります。
スタートアッププログラムの追加	不正なアプリケーションは、通常、Windows レジストリに自動スタートエントリを追加または変更して、コンピュータを起動するたびに自動的に起動します。

イベント監視で監視対象のシステムイベントを検出すると、そのイベントに設定された処理を実行します。

次の表は、管理者が監視対象のシステムイベントで実行できる処理の一覧を示します。

表 9-2. 監視対象のシステムイベントでの処理

処理	説明
診断	セキュリティエージェントは常にイベントに関連したプログラムの実行を許可し、診断用にイベントをログに記録します。 これは、すべての監視対象のシステムイベントのデフォルトの処理です。 **注意** このオプションは、64 ビットシステムのプログラムライブラリインジェクション (DLL インジェクション) イベントではサポートされていません。

処理	説明
許可	セキュリティエージェントは常にイベントに関連したプログラムの実行を許可します。
必要に応じて問い合わせ	セキュリティエージェントはイベントに関連したプログラムの実行を許可または拒否するように求めるメッセージを表示し、プログラムを除外リストに追加します。 特定の期間内にユーザが応答しない場合、セキュリティエージェントは自動的にプログラムの実行を許可します。デフォルトの期間は 30 秒です。 この時間を変更するには、423 ページの「グローバル挙動監視設定」を参照してください。 **注意** このオプションは、64 ビットシステムのプログラムライブラリインジェクション (DLL インジェクション) イベントではサポートされていません。
拒否	セキュリティエージェントは常にイベントに関連したプログラムの実行をブロックし、イベントをログに記録します。 通知が有効になっているプログラムをブロックした後、セキュリティエージェントはエンドポイントに通知を表示します。 通知の詳細については、425 ページの「セキュリティエージェントユーザへの挙動監視通知」を参照してください。

挙動監視除外リスト

挙動監視除外リストは、セキュリティエージェントが挙動監視を使用して監視しないプログラムのリストです。

- 承認済みプログラム: セキュリティエージェントは、[承認済みプログラム] リスト内のすべてのプログラムを挙動監視検索から除外します。

注意

挙動監視では [承認済みプログラム] リストに追加されたプログラムに対して処理を実行しませんが、他の検索機能 (ファイルベースの検索など) では引き続き、プログラムの実行を許可する前にそのプログラムを検索します。

- ブロックするプログラム: セキュリティエージェントは、[ブロックするプログラム] リスト内のプログラムをすべてブロックします。[ブロックするプログラム] リストを設定するには、イベント監視を有効にします。

除外リストは Web コンソールで設定します。また、セキュリティエージェントコンソールから独自の除外リストを設定する権限をユーザに付与することもできます。

詳細については、424 ページの「挙動監視権限」を参照してください。

除外リストでのワイルドカードのサポート

挙動監視の承認済みリストでは、ファイルパス、ファイル名、およびファイル拡張子の除外の種類の定義時にワイルドカード文字を使用できます。次の表を使用して除外リストの書式を適切に設定し、Apex One で正しいファイルとフォルダが検索から除外されるようにしてください。

サポートされるワイルドカード文字は次のとおりです。

- アスタリスク (*): 任意の文字または文字列を表します
- 疑問符 (?): 任意の 1 文字を表します

重要

挙動監視の承認済みリストでは、ワイルドカード文字を使用してシステムドライブの名称や UNC アドレスを置き換えることはできません。

除外の種類	ワイルドカードの使用法	一致する	一致しない
ディレクトリ	`C:\*` 指定したドライブにあるすべてのファイルとフォルダを除外します	• `C:¥sample.exe` • `C:¥folder¥test.doc`	• `D:¥sample.exe` • `E:¥folder¥test.doc`

除外の種類	ワイルドカードの使用法	一致する	一致しない
特定のフォルダ階層にある特定のファイル	`C:\*\Sample.exe` Sample.exe ファイルが C:¥ディレクトリのいずれかのサブフォルダにある場合にのみ除外します	• C:¥files¥Sample.exe • C:¥temp¥files¥Sample.exe	• C:¥sample.exe
UNC パス	`\\<UNC path>\*\Sample.exe` Sample.exe ファイルが指定した UNC パスのいずれかのサブフォルダにある場合にのみ除外します	• ¥¥<UNC path>¥files¥Sample.exe • ¥¥<UNC path>¥temp¥files¥Sample.exe	• R:¥files¥Sample.exe 理由: ネットワークドライブはサポートされていません。 • ¥¥<UNC path>¥Sample.exe 理由: ファイルが UNC パスのサブフォルダ内にありません。
ファイル名と拡張子	`C:\*.*` C:¥ディレクトリの任意のフォルダおよびサブフォルダにある、任意の拡張子のすべてのファイルを除外します	• C:¥Sample.exe • C:¥temp¥Sample.exe • C:¥test.doc	• D:¥sample.exe • C:¥Sample **注意** C:¥Sample にはファイル拡張子がないため、検索から除外されません。

除外の種類	ワイルドカードの使用法	一致する	一致しない
ファイル名	`C:\*.exe` C:¥ディレクトリの任意のフォルダおよびサブフォルダにある、拡張子が.exe のすべてのファイルを除外します	• C:¥Sample.exe • C:¥temp¥test.exe	• C:¥Sample.doc • C:¥temp¥test.bat • C:¥Sample **注意** C:¥Sample にはファイル拡張子がないため、検索から除外されません。
ファイル拡張子	`C:\Sample.*` C:¥ディレクトリにある、Sample という名前の任意の拡張子のすべてのファイルを除外します	• C:¥Sample.exe	• C:¥Sample1.doc • C:¥temp¥Sample.bat • C:¥Sample **注意** C:¥Sample にはファイル拡張子がないため、検索から除外されません。
特定のディレクトリ構造にあるファイル	`C:\*\*\Sample.exe` C:¥ディレクトリの第 2 階層以下のサブフォルダにある、ファイル名と拡張子が Sample.exe であるすべてのファイルを除外します	• C:¥files¥temp¥Sample.exe • C:¥files¥temp¥test¥Sample.exe	• C:¥Sample.exe • C:¥temp¥Sample.exe • C:¥files¥temp¥Sample.doc

除外の種類	ワイルドカードの使用法	一致する	一致しない
複雑なパスまたはファイル名	`C:\Sam*e??.exe` 名前が次の条件を満たすすべてのファイルを除外します • 先頭が「Sam」である • ファイル名の後ろから 3 文字目が「e」である • ファイル名の先頭の「Sam」と末尾の「e??」の間に少なくとも 1 文字ある • ファイル名の「e」からファイル拡張子までの間の文字数がちょうど 2 文字である • ファイル拡張子が.exe である すべての条件を満たすファイルが C:¥ディレクトリにある場合、そのファイルが挙動監視の検索から除外されます。	• C:¥Sample12.exe • C:¥SamSamSample12.exe	• C:¥SaSmple12.exe 理由: 先頭が「Sam」でありません • C:¥SamSamSam12.exe 理由: 後ろから 3 文字目が「e」でありません • C:¥Same12.exe 理由: 先頭の「Sam」と後ろから 3 文字目の「e」の間に文字がありません • C:¥Sample1.exe 理由:「e」から拡張子までの間の文字数が 2 文字でありません • C:¥Sample12.doc 理由: 拡張子が異なります

除外リストの環境変数のサポート

次の表は、リストにファイルまたはフォルダパスを追加するときに使用できる環境変数の一覧を示します。

環境変数	例	同等のパス
$allappdata$	$allappdata$\test\sample.exe	C:\ProgramData\test\sample.exe

環境変数	例	同等のパス
$allprograms$	$allprograms$\test\sample.exe	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\test\sample.exe
$programdir$	$programdir$\test\sample.exe	C:\Program Files\test\sample.exe
$programdirx86$	$programdirx86$\test\sample.exe	C:\Program Files (x86)\test\sample.exe
$rootdir$	$rootdir$\test\sample.exe	C:\test\sample.exe
$systemdir$	$systemdir$\test\sample.exe	C:\Windows\System32\test\sample.exe
$systemdirx86$	$systemdirx86$\test\sample.exe	C:\Windows\SysWOW64\test\sample.exe
$tempdir$	$tempdir$\test\sample.exe	C:\Windows\Temp\test\sample.exe
$userprofile$	$userprofile$\test\sample.exe	C:\user\{current_user_account}\test\sample.exe
$windir$	$windir$\test\sample.exe	C:\Windows\test\sample.exe

不正プログラム挙動ブロック、イベント監視、および除外リストの設定

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [挙動監視設定] の順にクリックします。
4. [ルール] タブをクリックします。
5. [不正プログラム挙動ブロック] セクションで、次の手順を実行します。

a. [不正プログラム挙動ブロックを有効にする] を選択し、ブロックする脅威の種類を指定します。

- 既知の脅威: 既知の不正プログラムの脅威に関連する挙動をブロックします。
- 既知の脅威と潜在的な脅威: 既知の脅威に関連付けられた挙動をブロックし、潜在的に不正な挙動に対して処理を実行します。

b. 有効にするランサムウェア対策オプションを選択します。

- 不正な暗号化や変更から文書を保護: 潜在的なランサムウェアによる文書の暗号化や変更を防止します。
  - 不審なプログラムによって変更されたファイルを自動的にバックアップして復元: ランサムウェアの脅威が検出された場合に、暗号化されたファイルのバックアップコピーをエンドポイントに作成してデータの損失を防止します。

注意

自動ファイルバックアップを実行するには、エージェントエンドポイントに 100MB 以上のディスク容量が必要です。また、バックアップされるのは 10MB 未満のファイルだけです。

- ランサムウェアに関連付けられていることの多いプロセスをブロック: 既知のランサムウェアに関連付けられているプロセスをブロックして、文書の暗号化や変更を防止します。
- プログラム検査を有効にして不正な実行可能ファイルを検出およびブロック: プログラム検査は、プロセスを監視して API フックを行うことで、予期しない挙動を示すプログラムを特定します。これにより、不正な実行可能ファイルの全体的な検出率が高くなりますが、システムのパフォーマンスが下がる場合があります。

ヒント

[ブロックする脅威] リストから [既知の脅威と潜在的な脅威] を選択すると、プログラム検査によるセキュリティが向上します。

詳細については、409 ページの「ランサムウェア対策」を参照してください。

c. [脆弱性対策] で [脆弱性攻撃に関連する異常な挙動を示すプログラムを終了] を有効にし、プログラムの潜在的な脆弱性を悪用した攻撃を防止します。

注意

脆弱性対策を使用するには、[プログラム検査を有効にして不正な実行可能ファイルを検出およびブロック] を選択する必要があります。

詳細については、411 ページの「脆弱性対策」を参照してください。

---

6. [新たに検出されたプログラム] セクションで、[Web またはメールアプリケーションチャネルを介してダウンロードされた新たなプログラムを監視する] を有効にし、ダウンロードされたプログラムの実行前にユーザにメッセージを表示するか、Apex One でログへの記録だけを行うかを選択します。

7. [イベント監視] セクションで、次の手順を実行します。

   a. [イベント監視を有効にする] を選択します。

   b. 監視するシステムイベントを選択し、選択したイベントごとに処理を選択します。

      監視対象のシステムイベントの詳細については、412 ページの「イベント監視」を参照してください。

8. [除外] タブをクリックし、除外リストを設定します。

   a. [プログラムのフルパスを入力してください] で、承認またはブロックするプログラムのフルパスを入力します。

   b. [承認済みリストに追加]、または [ブロックリストに追加] をクリックします。

   c. ブロックするプログラムまたは承認済みプログラムをリストから削除するには、プログラムの横にあるごみ箱アイコン () をクリックします。

注意

Apex One では、承認済みプログラムとブロックするプログラムを合計 1,024 個まで指定できます。

9. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。
   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
   - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

グローバル挙動監視設定

Apex One では、グローバルエージェント設定を、すべてのエージェントまたは特定の権限を持つエージェントにのみ適用します。

手順

1. [エージェント] > [グローバルエージェント設定] に移動します。
2. [セキュリティ設定] タブをクリックします。
3. [挙動監視設定] セクションに移動します。
4. 必要に応じて、[ユーザが次の時間以内に応答しない場合はプログラムの実行を許可する: __秒] を設定します。

   この設定は、イベント監視が有効で、監視対象のシステムイベントに対する処理が [必要に応じて問い合わせ] に設定されている場合にのみ機能します。このイベント処理では、イベントに関連するプログラムを許可するか、拒否するかを確認するメッセージがユーザに表示されます。一

定時間内にユーザが応答しない場合、プログラムが自動的に実行されます。

詳細については、412 ページの「イベント監視」を参照してください。

5. [システム] タブをクリックします。

6. [ソフトウェア安全性評価サービスの設定] セクションに移動し、ソフトウェア安全性評価サービスを必要に応じて有効にします。

   ソフトウェア安全性評価サービスでは、不正プログラム挙動ブロック、イベント監視、ファイアウォール、またはウイルス対策検索で検出されたプログラムに関するクエリがトレンドマイクロのデータセンターに送信され、プログラムの安全性が確認されます。ソフトウェア安全性評価サービスを有効にすることによって、誤検出の確率を低くすることができます。

   注意

   ソフトウェア安全性評価サービスを有効にする前に、セキュリティエージェントのプロキシ設定 (詳細については、687 ページの「セキュリティエージェントプロキシ設定」を参照) が正しく行われていることを確認してください。プロキシ設定の誤りやインターネット接続の中断は、トレンドマイクロのデータセンターから送信される応答の延期や不達の原因となり、監視対象のプログラムが応答していないように見えます。

   また、IPv6 セキュリティエージェントでは、トレンドマイクロのデータセンターに直接クエリを送信することはできません。このようなセキュリティエージェントがトレンドマイクロのデータセンターに接続できるようにするには、IP アドレスを変換可能な DeleGate などのデュアルスタックプロキシサーバが必要です。

7. [保存] をクリックします。

挙動監視権限

エージェントに挙動監視権限がある場合、セキュリティエージェントコンソールの [設定] 画面に [挙動監視] オプションが表示されます。そのため、ユーザは独自の除外リストを管理できます。

挙動監視権限の付与

手順

1. [エージェント] > [エージェント管理]に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [権限] タブの [挙動監視] セクションに移動します。
5. [セキュリティエージェントコンソールに挙動監視設定を表示] を選択します。
6. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。
   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
   - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

セキュリティエージェントユーザへの挙動監視通知

挙動監視によってプログラムがブロックされたらすぐに、Apex One からの通知メッセージをセキュリティエージェントコンピュータに表示できます。通

知メッセージの送信を有効にし、必要に応じてメッセージの内容を変更してください。

通知メッセージの送信の有効化

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [その他の設定] セクションタブをクリックし、[挙動監視設定] に移動します。
5. [プログラムをブロックした場合、通知を表示] を選択します。
6. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。
   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
   - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

通知メッセージの内容の変更

手順

1. [管理] > [通知] > [エージェント] に移動します。
2. [種類] のドロップダウンから、[挙動監視ポリシー違反] を選択します。
3. 表示されたテキストボックスで初期設定のメッセージを変更します。
   - 挙動監視ポリシー違反: 不正プログラム挙動ブロックでポリシー違反を検出したときにエンドユーザに通知するメッセージを指定します。
   - 新たに検出されたプログラム: 挙動ブロックで Web またはメールアプリケーションを介してダウンロードされた認識できないプログラムを検出したときにエンドユーザに通知するメッセージを指定します。
4. [保存] をクリックします。

挙動監視ログ

セキュリティエージェントでは、プログラムへの不正アクセスがログに記録され、サーバに送信されます。継続的に実行されているセキュリティエージェントではログが集約され、指定された時間間隔で送信されます。この間隔は初期設定では 1 時間です。

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログの削除スケジュールを設定します。ログの管理方法の詳細については、616 ページの「ログ管理」を参照してください。

挙動監視ログの表示

手順

1. [ログ] > [エージェント] > [セキュリティリスク] または [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [ログ] > [挙動監視ログ] または [ログの表示] > [挙動監視ログ] をクリックします。
4. ログの条件を指定して [ログを表示する] をクリックします。
5. ログが表示されます。ログには、次の情報が含まれています。
   - 日時
   - 不正プロセスが検出されたエンドポイント
   - エンドポイントのドメイン
   - 違反 (プロセスが違反しているイベント監視ルール)
   - 処理
   - イベント (プログラムがアクセスするオブジェクトの種類)
   - リスク
   - プログラム (不正プログラム)
   - 操作 (不正プログラムの実行処理)
   - 対象 (アクセスされたプロセス)
   - 脅威の感染経路
6. ログを CSV ファイルに保存するには、[CSV 形式ですべてエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。

挙動監視ログの送信スケジュールの設定

手順

1. <サーバインストールフォルダ>¥PCCSRV にアクセスします。
2. メモ帳などのテキストエディタを使用して、ofcscan.ini を開きます。
3. 文字列「SendBMLogPeriod」を検索し、その横の値を確認します。

   初期設定の 3,600 秒の場合、SendBMLogPeriod=3600 と記述されています。
4. この値は、秒数で指定します。

   たとえば、ログ期間を 2 時間に変更する場合、この値を 7200 に変更します。
5. ファイルを保存します。
6. [エージェント] > [グローバルエージェント設定] に移動します。
7. どの設定も変更せずに、[保存] をクリックします。
8. エージェントを再起動します。

第 10 章

デバイスコントロールの使用

この章では、デバイスコントロール機能を使用してコンピュータをセキュリティリスクから保護する方法について説明します。

この章は次のトピックで構成されます。

デバイスコントロール

デバイスコントロールは、コンピュータに接続されている外部のストレージデバイスやネットワークリソースへのアクセスを規制します。デバイスコントロール機能により、データの損失や漏えいを防ぐことができ、またファイル検索と併用することでセキュリティリスクからの保護が実現されます。

内部エージェントと外部エージェントに対してデバイスコントロールポリシーを設定できます。通常は、外部エージェントに対してより厳格なポリシーを設定します。

ポリシーは、Apex One エージェントツリーで細かく設定されます。特定のポリシーを、エージェントグループに適用したり、個別のエージェントに適用したりできます。また、単一のポリシーをすべてのエージェントに適用することもできます。

ポリシーが配信されると、エージェントは [エンドポイントの位置] 画面 (640 ページの「エンドポイント (コンピュータ)の位置」参照) で設定された位置の基準を使用して、その位置と適用されるポリシーを判断します。エージェントのポリシーは、位置が変わるたびに切り替えられます。

重要

- Windows Server では、いずれのバージョンでも初期設定でデバイスコントロールが無効になっています。これらのサーバプラットフォームに対してデバイスコントロールを有効にする前に、645 ページの「セキュリティエージェントサービス」で説明されているガイドラインとベストプラクティスをお読みください。
- サポートしているデバイスモデルの一覧については、情報漏えい対策オプションリストのドキュメントを参照してください。

  https://success.trendmicro.com/jp/solution/1312344

Apex One が監視できるデバイスの種類は、情報漏えい対策オプションライセンスがアクティベートされているかどうかによって異なります。情報漏えい対策オプションは個別にライセンスされるモジュールであり、使用する前にアクティベートする必要があります。情報漏えい対策オプションライセンスの詳細については、86 ページの「情報漏えい対策オプションライセンス」を参照してください。

表 10-1. 不正変更防止サービスで監視されるデバイス

デバイスの種類	デバイスの説明
ストレージデバイス	CD/DVD **重要** デバイスコントロールで制限できるのは、ライブファイルシステム形式を使用する CD/DVD 記憶デバイスへのアクセスだけです。マスター形式を使用する一部の他社製アプリケーションでは、デバイスコントロールを有効にしても引き続き読み取り/書き込み操作が可能な場合があります。フォーマットの種類に関係なく CD/DVD 記憶デバイスへのアクセスを制限するには、情報漏えい対策を使用します。 詳細については、484 ページの「データ記憶デバイス (CD/DVD) へのアクセスのブロック」を参照してください。
	フロッピーディスク
	ネットワークドライブ
	USB ストレージデバイス

表 10-2. 情報漏えい対策で監視されるデバイス

デバイスの種類	デバイスの説明
モバイルデバイス	モバイルデバイス
ストレージデバイス	CD/DVD
	フロッピーディスク
	ネットワークドライブ
	USB ストレージデバイス

デバイスの種類	デバイスの説明
非ストレージデバイス	Bluetooth アダプタ
	COM および LPT ポート
	IEEE 1394 インタフェース
	イメージングデバイス
	赤外線デバイス
	モデム
	PCMCIA カード
	Print Screen キー
	ワイヤレス NIC

ストレージデバイスに対する権限

ストレージデバイスに対するデバイスコントロール権限は、次の場合に使用されます。

- USB ストレージデバイス、CD/DVD、フロッピーディスク、およびネットワークドライブへのアクセスを許可する場合。これらのデバイスに対するフルアクセスを付与したり、アクセスレベルを制限したりすることができます。
- 承認済み USB ストレージデバイスのリストを設定する場合。デバイスコントロールでは、承認済みデバイスのリストに追加されている USB ストレージデバイスを除く、すべての USB ストレージデバイスへのアクセスをブロックできます。承認済みデバイスに対するフルアクセスを付与したり、アクセスレベルを制限したりすることができます。

次の表は、ストレージデバイスの権限をリストしたものです。

表 10-3. ストレージデバイスに対するデバイスコントロール権限

権限	デバイス上のファイル	受信ファイル
フルアクセス	許可される操作: コピー、移動、開く、保存、削除、実行	許可される操作: 保存、移動、コピー これは、デバイスにファイルを保存、移動、およびコピーできることを意味します。
変更	許可される操作: コピー、移動、開く、保存、削除 禁止される操作: 実行	許可される操作: 保存、移動、コピー
読み取りおよび実行	許可される操作: コピー、開く、実行 禁止される操作: 保存、移動、削除	禁止される操作: 保存、移動、コピー
読み取り	許可される操作: コピー、開く 禁止される操作: 保存、移動、削除、実行	禁止される操作: 保存、移動、コピー
デバイスの内容のみのリスト表示	禁止される操作: すべて デバイスおよびそれに含まれるファイルはユーザに (Windows Explorer などを使用して) 表示されます。	禁止される操作: 保存、移動、コピー
ブロック (情報漏えい対策オプションのインストール後に使用可能)	禁止される操作: すべて デバイスおよびそれに含まれるファイルはユーザに (Windows Explorer などを使用して) 表示されません。	禁止される操作: 保存、移動、コピー

ファイルベースの検索機能は、デバイスの権限を補完し、これらの権限よりも優先される場合があります。たとえば、権限ではファイルを開くことが可能でも、セキュリティエージェントによってファイルが不正プログラムに感染していることが検出された場合、不正プログラムを排除するために特定の検出時の処理がそのファイルに実行されます。検出時の処理が駆除の場合、

ファイルは駆除後に開かれます。ただし、検出時の処理が削除の場合、ファイルは削除されます。

ヒント

情報漏えい対策オプションのデバイスコントロールでは、すべての 64 ビットプラットフォームをサポートします。セキュリティエージェントでサポートされていないシステムで不正変更防止監視を行うには、デバイスの権限を「ブロック」に設定して、これらのデバイスへのアクセスを制限します。

ストレージデバイスに対する詳細な権限設定

詳細な権限設定は、ほとんどのストレージデバイスに対して制限された権限を付与する場合に適用されます。権限は次のいずれかになります。

- 変更
- 読み取りおよび実行
- 読み取り
- デバイスの内容のみのリスト表示

ストレージデバイスに対する権限を制限したまま、ストレージデバイスやローカルエンドポイント上の特定のプログラムに対する詳細な権限を付与することが可能です。

プログラムを定義するには、次のプログラムのリストを設定します。

表 10-4. プログラムのリスト

プログラムのリスト	説明	有効な入力
デバイスに対する読み取り/書き込みアクセス権のあるプログラム	このリストには、デバイスへの読み取りおよび書き込みアクセス権があるローカルプログラムおよびストレージデバイス上のプログラムを追加します。 ローカルプログラムには Microsoft Word (winword.exe) などがあり、このプログラムは通常 C:¥Program Files¥Microsoft Office¥Office にインストールされます。USB ストレージデバイスに対する権限が「デバイスの内容のみのリスト表示」でも、このリストに「C:¥Program Files¥Microsoft Office¥Office¥winword.exe」が含まれている場合は次の操作が可能です。 • ユーザは、Microsoft Word から USB ストレージデバイス上の任意のファイルに読み取りおよび書き込みアクセスを実行できます。 • ユーザは、Microsoft Word ファイルを USB ストレージデバイスに保存、移動、およびコピーできます。	プログラムのパスと名前 詳細については、438 ページの「デバイスコントロールの [許可されたプログラム] リストでのワイルドカードのサポート」を参照してください。
デバイス上の実行を許可されたプログラム	このリストには、ユーザまたはシステムによって実行可能なストレージデバイス上のプログラムを追加します。 たとえば、ユーザに CD からのソフトウェアのインストールを許可する場合は、「E:¥Installer¥Setup.exe」などインストールプログラムのパスと名前をこのリストに追加します。	プログラムのパスと名前、またはデジタル署名プロバイダ 詳細については、438 ページの「デバイスコントロールの [許可されたプログラム] リストでのワイルドカードのサポート」または 438 ページの「デジタル署名プロバイダの指定」を参照してください。

両方のリストにプログラムの追加が必要な場合があります。たとえば、USB ストレージデバイスのデータロック機能について考えます。この機能が有効

な場合は、デバイスのロックを解除する際、有効なユーザ名とパスワードを入力するよう求められます。データロック機能はデバイス上の「Password.exe」というプログラムを使用するため、ユーザがデバイスを正常にロック解除できるように、このプログラムを実行可能にする必要があります。また、「Password.exe」にデバイスへの読み取りおよび書き込みアクセスを与えて、ユーザがユーザ名とパスワードを変更できるようにする必要があります。

ユーザインタフェースでは、各リストに最大 100 個までプログラムを追加できます。

さらにプログラムをリストに追加したい場合は、それらを ofcscan.ini ファイルに追加する必要があります。このファイルには、最大 1,000 個までプログラムを追加できます。プログラムを ofcscan.ini ファイルに追加する手順については、446 ページの ofcscan.ini を使用したデバイスコントロールリストへのプログラムの追加を参照してください。

警告!

ofcscan.ini ファイルに追加されたプログラムはルートドメインに配信され、それによって個々のドメインやエージェントのプログラムが上書きされます。

デジタル署名プロバイダの指定

プロバイダから提供されるプログラムを信頼する場合は、デジタル署名プロバイダを指定します。たとえば、「Microsoft Corporation」、「Trend Micro, Inc.」のように入力します。デジタル署名プロバイダは、プログラムのプロパティで確認できます (たとえば、プログラムを右クリックして [プロパティ] を選択します)。

デバイスコントロールの [許可されたプログラム] リストでのワイルドカードのサポート

プログラムのパスと名前は 259 文字以内で指定する必要があり、英数字 (A～Z、a～z、0～9) のみを使用できます。プログラム名のみを指定することはできません。

ワイルドカード文字は、ドライブ文字およびプログラム名に使用できます。ドライブ文字など 1 文字のデータを表す場合は、疑問符 (?) を使用します。プ

ログラム名など複数文字のデータを表す場合は、アスタリスク (*) を使用します。

注意

フォルダ名にワイルドカードを使用することはできません。フォルダは正確な名前を指定する必要があります。

ワイルドカードの正しい使用例を次に示します。

表 10-5. ワイルドカードの正しい使用例

例	一致するデータ
?:\Password.exe	任意のドライブの直下にある「Password.exe」ファイル
C:\Program Files\Microsoft*.exe	C:\Program Files 内のファイル拡張子がある任意のファイル
C:\Program Files*.*	C:\Program Files 内のファイル拡張子がある任意のファイル
C:\Program Files\a?c.exe	C:\Program Files 内で、「a」で始まり「c」で終わる 3 文字の名前を持つ任意の.exe ファイル
C:*	ファイル拡張子に関係なく、C:\ドライブ直下の任意のファイル

ワイルドカードの間違った使用例を次に示します。

表 10-6. ワイルドカードの間違った使用例

例	理由
??:\Buffalo\Password.exe	?? は 2 文字を表しますが、ドライブ文字は 1 文字の英文字に限定されています。
*:\Buffalo\Password.exe	*は複数文字のデータを表しますが、ドライブ文字は 1 文字の英文字に限定されています。
C:*\Password.exe	フォルダ名にワイルドカードを使用することはできません。フォルダは正確な名前を指定する必要があります。
C:\?\Password.exe	

非ストレージデバイスの権限

非ストレージデバイスに対するアクセスは、許可またはブロックのいずれかになります。これらのデバイスに対して権限を細かく設定することはできません。

外部デバイスへのアクセスの管理 (情報漏えい対策オプションがアクティベートされている場合)

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [デバイスコントロール設定] の順にクリックします。
4. [外部エージェント] タブをクリックして外部エージェントの設定を行うか、[内部エージェント] タブをクリックして内部エージェントの設定を行います。
5. [デバイスコントロールを有効にする] を選択します。
6. 次のように設定を適用します。
   - [外部エージェント] タブで [内部エージェントにすべての設定を適用する] を選択すると、設定を内部エージェントに適用できます。
   - [内部エージェント] タブで [外部エージェントにすべての設定を適用する] を選択すると、設定を外部エージェントに適用できます。

   確認メッセージが表示されます。配信コマンドがすべてのエージェントに適用されるまでには、しばらく時間がかかります。
7. USB ストレージデバイスについて、自動実行機能 (`autorun.inf`) を許可するかブロックするかを選択します。

8. ストレージデバイスの設定を行います。

   a. 各ストレージデバイスの権限を選択します。

      権限の詳細については、434 ページの「ストレージデバイスに対する権限」を参照してください。

   b. USB ストレージデバイスに対する権限が [ブロック] の場合は、承認済みデバイスのリストを設定します。ユーザはこれらのデバイスに対するアクセスを許可され、管理者は、この権限を使用してユーザのアクセスレベルを制御できます。

      442 ページの「USB デバイスの承認済みリストの設定」を参照してください。

9. 非ストレージデバイスごとに、[許可] または [ブロック] を選択します。

10. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。

    - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
    - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

詳細な権限の設定

ユーザインタフェースでは特定のストレージデバイスに対して詳細な権限や通知を設定できますが、実際には、この権限や通知はすべてのストレージデバイスに適用されます。つまり、CD/DVD の [詳細な権限および通知] をクリックしても、実際には、すべてのストレージデバイスに対する権限と通知を定義することになります。

注意

詳細な権限や、プログラムに詳細な権限を正しく定義する方法については、436 ページの「ストレージデバイスに対する詳細な権限設定」を参照してください。

手順

1. [詳細な権限および通知] をクリックします。

   新しい画面が表示されます。

2. [ストレージデバイスに対する読み取り/書き込みアクセス権のあるプログラム] にプログラムのパスと名前を入力して、[追加] をクリックします。

   デジタル署名プロバイダは指定できません。

3. [ストレージデバイス上の実行を許可されたプログラム] にプログラムのパスと名前またはデジタル署名プロバイダを入力して、[追加] をクリックします。

4. [デバイスへの不正アクセスの検出時にエンドポイントに通知メッセージを表示] を選択します。

   - デバイスへの不正アクセスとは、禁止されるデバイス操作のことを指します。たとえば、デバイスの権限が「読み取り」の場合、そのデバイス上のファイルに対する保存、移動、削除、および実行の各操作は禁止されます。
   - 通知メッセージは変更できます。詳細については、447 ページの「デバイスコントロール通知の変更」を参照してください。

5. [戻る] をクリックします。

USB デバイスの承認済みリストの設定

USB デバイスの承認済みリストでは、アスタリスク (*) ワイルドカードを使用できます。任意のフィールドをアスタリスク (*) で置き換えると、他のフィールドを満たすデバイスをすべて含めることができます。たとえば [ベンダ]-

[モデル]-*は、シリアル ID に関係なく、指定したベンダの特定のモデルタイプのすべての USB デバイスを承認済みリストに配置します。

手順

1. [承認済みデバイス] をクリックします。
2. デバイスのベンダを入力します。
3. デバイスモデルとシリアル ID を入力します。

   ヒント

   デバイスリストツールは、エンドポイントに接続されたデバイスを照会する場合に使用します。このツールは、デバイスごとにデバイスのベンダ、モデル、およびシリアル ID を表示します。

4. デバイスの権限を選択します。

   権限の詳細については、434 ページの「ストレージデバイスに対する権限」を参照してください。

5. さらにデバイスを追加するには、プラス (+) アイコンをクリックします。
6. [< 戻る] をクリックします。

デバイスリストツール

エンドポイントに接続された外部デバイスを照会するには、エンドポイントごとにデバイスリストツールをローカルで実行します。このツールは、エンドポイントの外部デバイスを検索し、デバイス情報をブラウザ画面に表示します。この情報は、情報漏えい対策やデバイスコントロールのデバイス設定を指定するときに使用できます。

デバイスリストツールの実行

手順

1. デバイスリストツールを用意します。
   - Apex One サーバコンピュータで、<サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility¥ListDeviceInfo に移動します。
   - 対象エンドポイントにセキュリティエージェントがインストールされている場合は、C:¥Windows¥System32¥dgagent¥listDeviceInfo.exe に移動します。
2. listDeviceInfo.exe を対象のエンドポイントにコピーします。
3. エンドポイントで、listDeviceInfo.exe を実行します。
4. 表示されたブラウザ画面でデバイス情報を確認します。情報漏えい対策とデバイスコントロールでは次の情報が使用されます。
   - ベンダ (必須)
   - モデル (オプション)
   - シリアル ID (オプション)

外部デバイスへのアクセスの管理 (情報漏えい対策オプションがアクティベートされていない場合)

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [デバイスコントロール設定] の順にクリックします。

4. [外部エージェント] タブをクリックして外部エージェントの設定を行うか、[内部エージェント] タブをクリックして内部エージェントの設定を行います。
5. [デバイスコントロールを有効にする] を選択します。
6. 次のように設定を適用します。
   - [外部エージェント] タブで [内部エージェントにすべての設定を適用する] を選択すると、設定を内部エージェントに適用できます。
   - [内部エージェント] タブで [外部エージェントにすべての設定を適用する] を選択すると、設定を外部エージェントに適用できます。

   確認メッセージが表示されます。配信コマンドがすべてのエージェントに適用されるまでには、しばらく時間がかかります。
7. USB ストレージデバイスについて、自動実行機能 (autorun.inf) を許可するかブロックするかを選択します。
8. 各ストレージデバイスの権限を選択します。
9. ストレージデバイスに対する権限が次のいずれかの場合は、詳細な権限と通知を設定します。[変更]、[読み取りおよび実行]、[読み取り]、または [デバイスの内容のみのリスト表示]。

   441 ページの「詳細な権限の設定」を参照してください。
10. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。
    - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
    - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

ofcscan.ini を使用したデバイスコントロールリストへのプログラムの追加

注意

プログラムリストの詳細とこのリストに追加できるプログラムを正しく定義する方法については、436 ページの「ストレージデバイスに対する詳細な権限設定」を参照してください。

手順

1. Apex One サーバコンピュータで、<サーバインストールフォルダ>¥PCCSRV に移動します。
2. テキストエディタを使用して ofcscan.ini を開きます。
3. ストレージデバイスに対する読み取り/書き込みアクセス権のあるプログラムを追加するには、次の手順を実行します。
   a. 次の行を探します。

      ```
      [DAC_APPROVED_LIST]

      Count=x
      ```

   b. 「x」を、プログラムリストに含めるプログラム数に置き換えます。
   c. 「Count=x」の下に次の行を入力して、プログラムを追加します。

      ```
      Item<番号>=<プログラムのパスと名前、またはデジタル署名プロバイダ>
      ```

      次に例を示します。

      ```
      [DAC_APPROVED_LIST]

      Count=3

      Item0=C:¥Program Files¥program.exe

      Item1=?:¥password.exe

      Item2=Microsoft Corporation
      ```

4. ストレージデバイス上の実行を許可されたプログラムを追加するには、次の手順を実行します。

   a. 次の行を探します。

      ```
      [DAC_EXECUTABLE_LIST]

      Count=x
      ```

   b. 「x」を、プログラムリストに含めるプログラム数に置き換えます。

   c. 「Count=x」の下に次の行を入力して、プログラムを追加します。

      ```
      Item<番号>=<プログラムのパスと名前、またはデジタル署名プロバイダ>
      ```

      例:

      ```
      [DAC_EXECUTABLE_LIST]

      Count=3

      Item0=?:\Installer\Setup.exe

      Item1=E:\*.exe

      Item2=Trend Micro, Inc.
      ```

5. `ofcscan.ini` ファイルを保存して閉じます。

6. Apex One Web コンソールを開き、[エージェント] > [グローバルエージェント設定] の順に選択します。

7. [保存] をクリックして、プログラムリストをすべてのエージェントに配信します。

デバイスコントロール通知の変更

通知メッセージは、デバイスコントロール違反が発生したときにエンドポイントに表示されます。初期設定の通知メッセージは必要に応じて変更できます。

手順

1. [管理] > [通知] > [エージェント] に移動します。
2. [種類] のドロップダウンから、[デバイスコントロール違反] を選択します。
3. 表示されたテキストボックスで初期設定のメッセージを変更します。
4. [保存] をクリックします。

デバイスコントロールログ

セキュリティエージェントでは、デバイスへの不正アクセスがログに記録され、サーバに送信されます。継続的に実行されているエージェントではログが集約され、1 時間経過してから送信されます。再起動されたエージェントは、最後にログがサーバに送信された時刻を確認します。1 時間以上経過している場合は、ただちにエージェントからログが送信されます。

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログの削除スケジュールを設定します。ログの管理方法の詳細については、616 ページの「ログ管理」を参照してください。

デバイスコントロールログの表示

注意

ストレージデバイスにアクセスしようとした場合にのみログデータが生成されます。セキュリティエージェントは非ストレージデバイスへのアクセスを設定に従ってブロックまたは許可しますが、この処理はログに記録されません。

手順

1. [ログ] > [エージェント] > [セキュリティリスク] または [エージェント] > [エージェント管理] に移動します。

2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [ログ] > [デバイスコントロールログ] または [ログの表示] > [デバイスコントロールログ] をクリックします。
4. ログの条件を指定して [ログを表示する] をクリックします。
5. ログが表示されます。ログには、次の情報が含まれています。
   - 不正アクセスが検出された日時
   - 外部デバイスが接続されているかまたはネットワークリソースがマップされているエンドポイント
   - 外部デバイスが接続されているかまたはネットワークリソースがマップされているエンドポイントドメイン
   - アクセスされたデバイスの種類またはネットワークリソース
   - 対象 (アクセスされたデバイスまたはネットワークリソースのアイテム)
   - アクセス元 (アクセスが開始された場所)
   - 対象に設定されている権限
6. ログを CSV ファイルに保存するには、[CSV 形式ですべてエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。

第 11 章

情報漏えい対策の使用

この章では、情報漏えい対策機能の使用方法について説明します。

この章は次のトピックで構成されます。

情報漏えい対策

従来のセキュリティソリューションは、外部のセキュリティ上の脅威がネットワークに侵入するのを防ぐことに重点を置いていました。今日のセキュリティ環境では、それだけでは不十分です。デジタル資産と呼ばれる組織の機密データや重要データを権限のない部外者に公開するデータ侵害が頻繁に発生するようになりました。データ侵害は、社員の過失や不注意、データアウトソーシング、コンピューティングデバイスの盗難または紛失、不正な攻撃などが原因で発生します。

データ侵害の影響は次のとおりです。

- ブランドの評判に傷を付ける
- 組織に対する顧客の信頼を損ねる
- 問題を解決したり、規制違反の罰金を支払ったりするための余分なコストが発生する
- 知的財産が盗まれた場合にはビジネスチャンスや収益が失われる

データ侵害の流行や悪影響により、現在の組織は、デジタル資産保護をセキュリティインフラストラクチャの必須要素と見なしています。

情報漏えい対策は、組織の機密データを不慮の流失や意図的な漏えいから守ります。情報漏えい対策により、管理者は次のことを実行できます。

- データ識別子を使用して保護する必要がある機密情報の識別
- メールや外部デバイスなどの一般的な転送チャネルを通したデジタル資産の転送を制限または阻止するポリシーの作成
- 制定されたプライバシー標準へのコンプライアンスの実施

機密情報の漏えいの危険性を監視するには、まず次の点について確認する必要があります。

- どのデータを無許可のユーザから保護する必要があるか。
- 機密データはどこにあるか。
- 機密データはどのような方法で送受信されるか。

- どのユーザが機密データへのアクセスや機密データの送信を許可されているか。
- セキュリティの違反が発生した場合にどのような処理を実行する必要があるか。

この重要な監査では、通常は、複数の部署や、組織の機密情報に詳しいユーザを対象にします。

機密情報とセキュリティポリシーをすでに定義している場合は、データ識別子と企業ポリシーの定義を始めることができます。

情報漏えい対策のポリシー

Apex One は、情報漏えい対策ポリシーで定義された一連のルールに照らしてファイルまたはデータを評価します。ポリシーによって、不正な転送から保護する必要があるファイルやデータが判別され、転送の検出時に Apex One で実行する処理が決定されます。

注意

Apex One では、サーバとセキュリティエージェント間のデータ送信は監視されません。

ポリシーは、内部と外部のセキュリティエージェントに対して設定できます。通常は、外部エージェントに対してより厳格なポリシーを設定します。

ポリシーは、エージェントグループまたは個別のエージェントに適用できます。

ポリシーが配信されると、エージェントは エンドポイントの位置 (640 ページの「エンドポイント (コンピュータ)の位置」を参照) で設定した位置基準を使用して、正しい位置設定と適用されるポリシーを判断します。エージェントは位置が変化するたびにポリシーを切り替えます。

ポリシー設定

情報漏えい対策ポリシーを定義するには、次の設定を行って、その設定を選択したエージェントに配信します。

表 11-1. 情報漏えい対策ポリシーを定義する設定

設定	説明
ルール	情報漏えい対策ルールには複数のテンプレート、チャネル、処理を含むことができます。各ルールは、ルールを包含する情報漏えい対策ポリシーのサブセットです。 **注意** 情報漏えい対策は優先順位に従ってルールおよびテンプレートを処理します。ルールが「放置 (ログのみ)」に設定されている場合、情報漏えい対策はリスト内の次のルールを処理します。ルールが「ブロック」または「理由申請」に設定されている場合、情報漏えい対策はユーザ処理をブロックまたは承認し、そのルール/テンプレートをそれ以上処理しません。
テンプレート	情報漏えい対策テンプレートは、データ ID と論理演算子 (And、Or、Except) を組み合わせて条件文を形成します。特定の条件文を満たすファイルまたはデータだけに、情報漏えい対策ルールが適用されます。 情報漏えい対策には事前定義済みのテンプレートが付属しており、管理者はテンプレートをカスタマイズして使用できます。 情報漏えい対策ルールには、1 つまたは複数のテンプレートを含めることができます。情報漏えい対策では、テンプレートのチェック時に初回一致ルールが使用されます。これは、特定のファイルまたはデータがテンプレート内のデータ ID に一致すると、それ以上他のテンプレートがチェックされないことを意味します。
チャネル	チャネルは、機密情報を送信するエンティティです。情報漏えい対策では、メール、リムーバブルストレージデバイス、インスタントメッセンジャーアプリケーションなど、一般的な送信チャネルがサポートされます。
処理	情報漏えい対策は、任意のチャネルを通じて機密情報の転送が検出されたときに、1 つ以上の処理を実行します。

設定	説明
除外	除外は、設定された情報漏えい対策ルールよりも優先されます。除外の設定により、監視対象外、監視対象、および圧縮ファイル検索の管理を行います。
データ識別子	情報漏えい対策では、データ識別子を使用して機密情報を識別します。データ識別子には、パターン、ファイル属性、キーワードなどがあり、これらが情報漏えい対策テンプレートの基盤となります。

データ識別子の種類

デジタル資産とは、組織で保護する必要のあるファイルやデータを意味します。デジタル資産は次のデータ識別子を使用して定義することができます。

- パターン: 特定の構造を持つデータ。

  詳細については、455 ページの「パターン」を参照してください。

- ファイル属性: ファイルの種類やサイズなどのファイルのプロパティ。

  詳細については、460 ページの「ファイル属性」を参照してください。

- キーワードリスト: 特別な単語や語句のリスト。

  詳細については、463 ページの「キーワード」を参照してください。

注意

情報漏えい対策テンプレートで使用されているデータ識別子を削除することはできません。データ識別子を削除する前にテンプレートを削除してください。

パターン

パターンは特定の構造を持つデータです。たとえば、クレジットカード番号の多くは 16 桁の「nnnn-nnnn-nnnn-nnnn」という形式で表現されるため、パターンによる検出に適しています。

事前定義済みのパターンとカスタマイズしたパターンを使用できます。

詳細については、456 ページの「事前定義済みのパターン」および 456 ページの「カスタマイズしたパターン」を参照してください。

事前定義済みのパターン

情報漏えい対策には、事前定義済みのパターンが付属しています。これらのパターンは、変更や削除ができません。

これらのパターンは、パターンマッチングと数学的な等式を使用して検証されます。機密と考えられるデータがパターンに一致すると、そのデータに対してさらに検証チェックが実行されることもあります。

事前定義済みのパターンの全リストについては、情報漏えい対策オプションリストのドキュメントを参照してください。

https://success.trendmicro.com/jp/solution/1312344

事前定義済みのパターンの設定の表示

注意

事前定義済みのパターンは、変更や削除ができません。

手順

1. [エージェント] > [情報漏えい対策] > [データ識別子] に移動します。
2. [パターン] タブをクリックします。
3. パターン名をクリックします。
4. 開いた画面で設定を確認します。

カスタマイズしたパターン

事前定義済みパターンに該当しないパターンを利用したい場合は、カスタマイズしたパターンを作成し、利用する事が出来ます。

パターンは強力な文字列照合ツールです。パターンを作成する前に、以下の注意点をご確認ください。パターンの善し悪しが性能に大きく影響する場合があります。

パターンを作成する際の注意:

- 有効なパターンを定義するための参考として事前定義済みのパターンを参照してください。たとえば、日付を含むパターンを作成する場合は、「日付」に事前定義されたパターンを参照してください。
- 情報漏えい対策は Perl 互換正規表現 (PCRE) で定義されたパターン形式に準拠しています。PCRE の詳細については、次の Web サイトを参照してください。

  http://www.pcre.org/
- 単純なパターンから始めてください。不正なアラームが発生した場合にパターンを修正したり、検出率を高めるためにパターンを調整したりします。

パターンを作成するときには、いくつかの条件の中から選択できます。パターンに選択した条件を満たすデータだけが、情報漏えい対策ポリシーの適用対象となります。各条件オプションの詳細については、457 ページの「カスタマイズしたパターンの条件」を参照してください。

カスタマイズしたパターンの条件

表 11-2. カスタマイズしたパターンの条件オプション

条件	ルール	例
なし	-	すべて: 米国勢調査局発行の名前 • パターン:[^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]

条件	ルール	例
特定の文字	パターンには、指定した文字が含まれている必要があります。 さらに、パターンの文字数は、最小文字数以上、最大文字数以下である必要があります。	米国 - ABA 銀行ルーティング番号 • パターン:[^\d]([0123678]\d{8})[^\d] • 文字: 0123456789 • 最小文字数: 9 • 最大文字数: 9
サフィックス	サフィックスはパターンの最終セグメントを意味します。サフィックスには、指定された文字と特定の文字数が含まれている必要があります。 さらに、パターンの文字数は、最小文字数以上、最大文字数以下である必要があります。	すべて - 自宅住所 • パターン:\D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave|road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.?[0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\ s\d{5}(-\d{4})?)[^\d-] • サフィックス文字: 0123456789- • 文字数: 5 • パターンの最小文字数: 25 • パターンの最大文字数: 80
単一のセパレータ文字	パターンは 2 つのセグメントで構成し、1 つの文字で区切る必要があります。文字は 1 バイト長にする必要があります。 さらに、セパレータ文字の左側の文字数は下限値と上限値の範囲に収める必要があります。セパレータ文字の右側の文字数は上限値を超えないようにする必要があります。	すべて - メールアドレス • パターン:[^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] • セパレータ: @ • 左側の最小文字数: 3 • 左側の最大文字数: 15 • 右側の最大文字数: 30

カスタマイズしたパターンの作成

手順

1. [エージェント] > [情報漏えい対策] > [データ識別子] に移動します。
2. [パターン] タブをクリックします。
3. [追加] をクリックします。

   新しい画面が表示されます。
4. パターンの名前を入力します。名前は、100 バイト以下の長さにする必要があり、次の文字を含めることができません。

   - > < * ^ | & ? \ /
5. 長さが 256 バイトを超えない説明を入力してください。
6. 表示するデータを入力します。

   たとえば、ID 番号に関するパターンを作成する場合は、サンプル ID 番号を入力します。このデータは、参照目的にのみ使用し、製品内の他の場所には表示されません。
7. 次の条件のいずれかを選択して、その条件に合わせて追加の設定値を指定します (457 ページの「カスタマイズしたパターンの条件」を参照)。

   - なし
   - 特定の文字
   - サフィックス
   - 単一のセパレータ文字
8. 実際のデータでパターンをテストします。

   [テストデータ] テキストボックスに有効な値を入力して [テスト] をクリックし、結果を確認します。
9. 目的の結果であれば、[保存] をクリックします。

注意

テストが成功した場合にのみ設定を保存します。データを検出できないパターンは、システムリソースを浪費し、性能に影響を与える可能性があります。

10. 設定をエージェントに配信するよう指示するメッセージが表示されます。[閉じる] をクリックします。
11. 情報漏えい対策データ識別子 画面に戻って、[すべてのエージェントに適用] をクリックします。

カスタマイズしたパターンのインポート

このオプションは、パターンを含んだ適切な形式の.dat ファイルがある場合に使用します。このファイルは、現在アクセスしているサーバまたは別のサーバからパターンをエクスポートすることによって作成できます。

手順

1. [エージェント] > [情報漏えい対策] > [データ識別子] に移動します。
2. [パターン] タブをクリックします。
3. [インポート] をクリックしてから、パターンが保存された.dat ファイルを選択します。
4. [開く] をクリックします。

   インポートが成功したかどうかを示すメッセージが表示されます。インポートするパターンがすでに存在する場合は省略されます。
5. [すべてのエージェントに適用] をクリックします。

ファイル属性

ファイル属性はファイル独自のプロパティです。データ識別子を定義するときに、ファイルタイプとファイルサイズという 2 つのファイル属性を使用できます。たとえば、ソフトウェア開発会社では、会社のソフトウェアインス

トーラの共有を、ソフトウェアの開発とテストを担当している開発部門に制限しなければならない場合があります。この場合は、Apex One 管理者はポリシーを作成して、サイズが 10～40MB の実行可能ファイルが開発以外の部門に転送されるのをブロックできます。

ファイル属性自体は、機密ファイルの識別子に適しているとは言えません。このトピックの例では、他の部門で共有されているサードパーティ製ソフトウェアがブロックされる可能性があります。そのため、ファイル属性と他の情報漏えい対策データ識別子を組み合わせて、機密ファイルの検出対象を絞り込むことをお勧めします。

サポートされるファイルタイプの全リストについては、情報漏えい対策オプションリストのドキュメントを参照してください。

https://success.trendmicro.com/jp/solution/1312344

事前定義済みのファイル属性リスト

情報漏えい対策には、事前定義済みのファイル属性リストが付属しています。このリストは、変更や削除ができません。リストにはそれぞれ固有の条件が組み込まれており、テンプレートに照らしてポリシー違反と見なすかどうかを判別します。

事前定義済みのファイル属性リストは、CD/DVD へのアクセスを制限する場合に使用します。

詳細については、484 ページの「データ記憶デバイス (CD/DVD) へのアクセスのブロック」を参照してください。

ファイル属性リストの作成

手順

1. [エージェント] > [情報漏えい対策] > [データ識別子] に移動します。
2. [ファイル属性] タブをクリックします。
3. [追加] をクリックします。

   新しい画面が表示されます。

4. ファイル属性リストの名前を入力します。名前は、100 バイト以下の長さにする必要があり、次の文字を含めることができません。

   - > < * ^ | & ? \ /

5. 長さが 256 バイトを超えない説明を入力してください。

6. 目的の実際のファイルタイプを選択します。

7. 含めるファイルタイプがリストに掲載されていない場合は、[ファイル拡張子] を選択し、そのファイルタイプの拡張子を入力します。情報漏えい対策は、実際のファイルタイプではなく指定されたファイル拡張子をチェックします。ファイル拡張子を指定する際のガイドライン:

   - 各拡張子の先頭にはアスタリスク (*) とピリオド (.) を付け、その後に拡張子を指定する必要があります。アスタリスクはワイルドカードであり、ファイルの実際の名前を表しています。たとえば、`*.pol` は `12345.pol` や `test.pol` と一致します。

   - 拡張子にワイルドカードを含めることができます。1 文字のデータを表す場合は疑問符 (?) を使用し、複数の文字を表す場合はアスタリスク (*) を使用します。次の例を参照してください。

     - `*.*m` は、`ABC.dem`、`ABC.prm`、`ABC.sdcm` などのファイルと一致します。

     - `*.m*r` は、`ABC.mgdr`、`ABC.mtp2r`、`ABC.mdmr` などのファイルと一致します。

     - `*.fm?`は、`ABC.fme`、`ABC.fml`、`ABC.fmp` などのファイルと一致します。

   - 拡張子の末尾にアスタリスクを追加すると、ファイル名や関係のない拡張子の一部と一致する可能性があるので注意してください。例:`*.do*`は、`abc.doctor_john.jpg` や `abc.donor12.pdf` と一致します。

   - 複数のファイル拡張子はセミコロン (;) で区切って入力してください。セミコロンの後に空白を追加する必要はありません。

8. 最小ファイルサイズと最大ファイルサイズをバイト単位で入力します。両方のファイルサイズは、0 より大きい整数にする必要があります。

9. [保存]をクリックします。
10. 設定をエージェントに配信するよう指示するメッセージが表示されます。[閉じる] をクリックします。
11. 情報漏えい対策データ識別子 画面に戻って、[すべてのエージェントに適用] をクリックします。

ファイル属性リストのインポート

このオプションは、ファイル属性リストを含んだ適切な形式の.dat ファイルがある場合に使用します。このファイルは、現在アクセスしているサーバまたは別のサーバからファイル属性リストをエクスポートすることによって作成できます。

手順

1. [エージェント] > [情報漏えい対策] > [データ識別子] に移動します。
2. [ファイル属性] タブをクリックします。
3. [インポート] をクリックしてから、ファイル属性リストが保存された.dat ファイルを選択します。
4. [開く] をクリックします。

   インポートが成功したかどうかを示すメッセージが表示されます。インポートするファイル属性リストがすでに存在する場合は省略されます。
5. [すべてのエージェントに適用] をクリックします。

キーワード

キーワードは特殊な単語または語句です。関連するキーワードをキーワードリストに追加することで、特定の種類のデータを識別できます。たとえば、「予後」、「血液型」、「予防接種」、および「医師」は診断書で使用されるキーワードです。診断書ファイルの転送を禁止したい場合は、情報漏えい対策ポリシーでこれらのキーワードを使用し、これらのキーワードを含むファイルをブロックするように情報漏えい対策を設定できます。

よく使用される単語を組み合わせて意味のあるキーワードを形成できます。たとえば、「end」、「read」、「if」、および「at」を組み合わせて、「END-IF」、「END-READ」、「AT END」などのソースコードで見られるキーワードを形成できます。

事前定義済みのキーワードリストとカスタマイズしたキーワードリストを使用できます。詳細については、464 ページの「事前定義済みのキーワードリスト」および 465 ページの「カスタマイズしたキーワードリスト」を参照してください。

事前定義済みのキーワードリスト

情報漏えい対策には、事前定義済みのキーワードリストが付属しています。これらのキーワードリストは、変更や削除ができません。リストにはそれぞれ固有の条件が組み込まれており、テンプレートに照らしてポリシー違反と見なすかどうかを判別します。

情報漏えい対策の事前定義済みキーワードリストの詳細については、情報漏えい対策オプションリストのドキュメントを参照してください。

https://success.trendmicro.com/jp/solution/1312344

キーワードリストの機能

キーワード数の条件

キーワードリストにはそれぞれ条件が含まれており、一定数のキーワードがドキュメントに存在すると、リストに照らして違反と見なされます。

キーワード数の条件には、次の値が含まれます。

- すべて:ドキュメントに、リスト内のすべてのキーワードが存在する必要があります。
- いずれか:ドキュメントに、リスト内のキーワードがいずれか 1 つ存在する必要があります。

- 特定の数:ドキュメントに、少なくとも指定された数のキーワードが存在する必要があります。ドキュメント内のキーワードが指定された数より多い場合、違反と見なされます。

距離条件

一部のリストには、違反があるかどうかを判別する「距離」条件が含まれています。「距離」とは、あるキーワードの最初の文字と、別のキーワードの最初の文字との間の文字数を表します。次のエントリについて考えます。

First Name:_John_ Last Name:_Smith_

[フォーム - 名、姓] リストには、50 文字の「距離」条件と、代表的なフォームフィールド「名」と「姓」が含まれています。上記の例では、「First Name」の「F」と「Last Name」の「L」の間の文字数が 18 なので、違反と見なされます。

違反と見なされないエントリの例は、次のとおりです。

The first name of our new employee from Switzerland is John.His last name is Smith.

この例では、「first name」の「f」と「last name」の「l」の間の文字数は 61 です。この場合は距離のしきい値を超えるので、違反とは見なされません。

カスタマイズしたキーワードリスト

どの事前定義済みのキーワードリストも要件を満たさない場合は、カスタマイズしたキーワードリストを作成します。

キーワードリストを設定するときに選択可能な条件がいくつかあります。キーワードリストは、情報漏えい対策によるポリシーの適用に関係なく、選択した条件を満たす必要があります。キーワードリストごとに次の条件のいずれかを選択します。

- いずれかのキーワード
- すべてのキーワード
- <x> 文字以下のすべてのキーワード

- キーワードの合計スコアがしきい値を超過

条件のルールの詳細については、466 ページの「カスタマイズしたキーワードリストの条件」を参照してください。

カスタマイズしたキーワードリストの条件

表 11-3. キーワードリストに関する条件

条件	ルール
いずれかのキーワードと一致	ファイルには、キーワードリスト内の 1 つ以上のキーワードが含まれている必要があります。
すべてのキーワード	ファイルには、キーワードリスト内のすべてのキーワードが含まれている必要があります。
<x> 文字以下のすべてのキーワード	ファイルには、キーワードリスト内のすべてのキーワードが含まれている必要があります。さらに、あるキーワードから次のキーワードまでの長さが<x>文字以内である必要があります。 たとえば、WEB、DISK、および USB の 3 つのキーワードがあり、指定した文字数が 20 であるとします。 情報漏えい対策で DISK、WEB、USB の順ですべてのキーワードが検出された場合は、「D」(DISK) から「W」(WEB) までの文字数と「W」から「U」(USB) の文字数が 20 文字以下である必要があります。 次のデータはこの条件を満たします。DISK####WEB############USB 次のデータはこの条件を満たしません。 DISK******************WEB****USB (「D」と「W」の間が 23 文字) この文字数を小さくすると (10 など) 検索時間は短くなりますが、検出範囲は制限される傾向にあります。これは、特に大きなファイルで、機密データが検出される確率が低下します。数字を大きくするほど、対象範囲も広がりますが、検索時間は長くなります。

条件	ルール
キーワードの合計スコアがしきい値を超過	ファイルには、キーワードリスト内の 1 つ以上のキーワードが含まれている必要があります。1 つのキーワードしか検出されなかった場合は、そのスコアがしきい値を上回っている必要があります。複数のキーワードが存在する場合は、それらの合計スコアがしきい値を上回っている必要があります。 キーワードごとに 1 ～ 10 のスコアを割り当てます。人事部門での「昇給」など、機密性の高い単語または語句には比較的高いスコアを割り当てる必要があります。それ自体にあまり意味のない単語または語句には低いスコアを割り当てることができます。 しきい値を設定するときに、キーワードに割り当てたスコアを考慮します。たとえば、5 つのキーワードがあり、そのうちの 3 つのキーワードの優先順位が高い場合は、しきい値を優先順位の高い 3 つのキーワードの合計スコア以下にします。これは、ファイルからこの 3 つのキーワードが検出された場合に、機密扱いの対象として十分であることを意味します。

キーワードリストの作成

手順

1. [エージェント] > [情報漏えい対策] > [データ識別子] に移動します。
2. [キーワードリスト] タブをクリックします。
3. [追加] をクリックします。

   新しい画面が表示されます。
4. キーワードリストの名前を入力します。名前は、200 バイト以下の長さにする必要があり、次の文字を含めることができません。

   - > < * ^ | & ? \ /
5. 長さが 256 バイトを超えない説明を入力してください。
6. 次の条件のいずれかを選択して、その条件に合わせて追加の設定値を指定します。

   - 任意のキーワード

- すべてのキーワード
- <x> 文字以下のすべてのキーワード
- キーワードの合計スコアがしきい値を超過

7. キーワードを手動でリストに追加するには

   a. 長さが 3 ～ 40 バイトのキーワードを入力して、大文字と小文字を区別するかどうかを指定します。

   b. [追加] をクリックします。

8. [インポート] オプションを使用してキーワードを追加するには

   注意

   このオプションは、キーワードを含んだ適切な形式の.csv ファイルがある場合に使用します。このファイルは、現在アクセスしているサーバまたは別のサーバからキーワードをエクスポートすることによって作成できます。

   a. [インポート] をクリックしてから、キーワードが保存された.csv ファイルを選択します。

   b. [開く] をクリックします。

      インポートが成功したかどうかを示すメッセージが表示されます。インポートするキーワードがすでにリスト内に存在する場合は省略されます。

9. キーワードを削除するには、そのキーワードを選択して、[削除] をクリックします。

10. キーワードをエクスポートするには

    注意

    [エクスポート] 機能は、キーワードをバックアップするか、キーワードを別のサーバにインポートする場合に使用します。キーワードリスト内のすべてのキーワードがエクスポートされます。キーワードを個別にエクスポートすることはできません。

a. [エクスポート] をクリックします。

b. 生成された.csv ファイルを任意の場所に保存します。

11. [保存]をクリックします。

12. 設定をエージェントに配信するよう指示するメッセージが表示されます。[閉じる] をクリックします。

13. 情報漏えい対策データ識別子 画面に戻って、[すべてのエージェントに適用] をクリックします。

キーワードリストのインポート

このオプションは、キーワードリストを含んだ適切な形式の.dat ファイルがある場合に使用します。このファイルは、現在アクセスしているサーバまたは別のサーバからキーワードリストをエクスポートすることによって作成できます。

手順

1. [エージェント] > [情報漏えい対策] > [データ識別子] に移動します。
2. [キーワード] タブをクリックします。
3. [インポート] をクリックしてから、キーワードリストが保存された.dat ファイルを選択します。
4. [開く] をクリックします。

   インポートが成功したかどうかを示すメッセージが表示されます。インポートするキーワードリストがすでに存在する場合は省略されます。
5. [すべてのエージェントに適用] をクリックします。

情報漏えい対策テンプレート

情報漏えい対策テンプレートは、情報漏えい対策データ識別子と、条件文を形成する論理演算子 (および、または、除外) で構成されます。特定の条件文

を満たすファイルやデータのみが情報漏えい対策ポリシーの対象となります。

たとえば、「雇用契約」ポリシーの対象ファイルの条件を、「Microsoft Word ファイル (ファイル属性)」および「特定の法律用語を含む (キーワード)」および「ID 番号を含む (パターン)」のように指定できます。このポリシーを使用すれば、人事担当者が印刷処理を介してファイルを転送できるため、従業員がそのハードコピーに署名できます。メールなどの他の使用可能なチャネル経由の転送はすべてブロックされます。

情報漏えい対策データ識別子の定義が完了していれば、独自のテンプレートを作成できます。事前定義済みのテンプレートを使用することもできます。詳細については、471 ページの「カスタマイズした情報漏えい対策テンプレート」および 470 ページの「事前定義済みの情報漏えい対策テンプレート」を参照してください。

注意

情報漏えい対策ポリシーで使用されているテンプレートを削除することはできません。テンプレートを削除する前にポリシーからテンプレートを削除します。

事前定義済みの情報漏えい対策テンプレート

情報漏えい対策には、次のように、さまざまな規制基準に準拠するために使用可能な事前定義済みのテンプレートが付属しています。これらのテンプレートは、変更や削除ができません。

- GLBA:Gramm-Leach-Billey Act
- HIPAA:Health Insurance Portability and Accountability Act (医療保険の相互運用性と説明責任に関する法律)
- PCI-DSS:Payment Card Industry Data Security Standard (PCI-DSS: カード会員データや取引情報を保護することを目的に作成されたクレジット業界のセキュリティ基準)
- SB-1386:US Senate Bill 1386
- US PII:United States Personally Identifiable Information (米国で個人を特定できる情報)

すべての事前定義済みのテンプレートの目的の一覧、および保護されるデータの例については、情報漏えい対策オプションリストのドキュメントを参照してください。

https://success.trendmicro.com/jp/solution/1312344

カスタマイズした情報漏えい対策テンプレート

データ識別子の定義が完了したら、独自のテンプレートを作成します。テンプレートは、データ識別子と、条件文を形成する論理演算子 (And、Or、Except) で構成されます。

条件文と論理演算子の働きと例については、471 ページの「条件文と論理演算子」を参照してください。

条件文と論理演算子

情報漏えい対策は左から右に条件文を評価します。条件文を設定する場合は、論理演算子を慎重に使用してください。論理演算子を間違って使用すると、予期せぬ結果をもたらす不正な条件文になります。

次の表の例を参照してください。

表 11-4. サンプル条件文

条件文	説明と例
[データ識別子 1] および [データ識別子 2] 除外 [データ識別子 3]	ファイルは、[データ識別子 1] と [データ識別子 2] の条件を満たすが、[データ識別子 3] の条件を満たしていない必要があります。 次に例を示します。 ファイルは、[Adobe PDF 文書] であり、[メールアドレス] を含むが、[キーワードリスト内のすべてのキーワード] を含まない必要があります。

条件文	説明と例
[データ識別子 1] または [データ識別子 2]	ファイルは [データ識別子 1] または [データ識別子 2] の条件を満たす必要があります。 例: ファイルは、[Adobe PDF 文書] であるか、[Microsoft Word ドキュメント] である必要があります。
除外 [データ識別子 1]	ファイルは [データ識別子 1] の条件を満たしていない必要があります。 例: ファイルは [マルチメディアファイル] 以外である必要があります。

表の最後の例で示したように、ファイルが条件文内のいずれのデータ識別子の条件も満たさないことが必要な場合は、条件文内の最初のデータ識別子に「除外」演算子を使用できます。ただし、ほとんどの場合、最初のデータ識別子に演算子は使用しません。

テンプレートの作成

手順

1. [エージェント] > [情報漏えい対策] > [情報漏えい対策テンプレート] に移動します。
2. [追加] をクリックします。

   新しい画面が表示されます。
3. テンプレートの名前を入力します。名前は、200 バイト以下の長さにする必要があり、次の文字を含めることができません。

   - > < * ^ | & ? \ /
4. 長さが 256 バイトを超えない説明を入力してください。
5. データ識別子を選択してから、[追加] アイコンをクリックします。

   定義を選択する場合:

- 複数のエントリを選択するには、<Ctrl> キーを押しながらデータ識別子を選択します。
- 検索機能は、特定の定義を想定している場合に使用します。データ識別子名のすべてまたは一部を入力できます。
- テンプレートごとに最大 30 のデータ識別子を含めることができます。

6. 新しいパターンを作成するには、[パターン] をクリックし、[新しいパターンの追加] をクリックします。表示された画面で、パターンを設定します。
7. 新しいファイル属性リストを作成するには、[ファイル属性] をクリックし、[新しいファイル属性の追加] をクリックします。表示された画面で、ファイル属性リストを設定します。
8. 新しいキーワードリストを作成するには、[キーワード] をクリックし、[新しいキーワードの追加] をクリックします。表示された画面で、キーワードリストを設定します。
9. パターンを選択した場合は、出現頻度を入力します。情報漏えい対策がパターンをポリシーの対象とするには、指定された回数だけ出現している必要があります。
10. 定義ごとに論理演算子を選択します。

注意

条件文を設定する場合は、論理演算子を慎重に使用してください。論理演算子を間違って使用すると、予期せぬ結果をもたらす不正な条件文になります。正しい使用例については、471 ページの「条件文と論理演算子」を参照してください。

---

11. 選択したデータ識別子のリストからデータ識別子を削除するには、ごみ箱アイコンをクリックします。
12. [プレビュー] で、条件文を確認し、目的の記述と異なる場合は変更します。
13. [保存]をクリックします。

14. 設定をエージェントに配信するよう指示するメッセージが表示されます。[閉じる] をクリックします。

15. 情報漏えい対策テンプレート 画面に戻って、[すべてのエージェントに適用] をクリックします。

テンプレートのインポート

このオプションは、正しくフォーマットされた.dat ファイルにテンプレートが保存されている場合に使用します。このファイルは、現在アクセスしているサーバまたは別のサーバからテンプレートをエクスポートすることによって作成できます。

手順

1. [エージェント] > [情報漏えい対策] > [情報漏えい対策テンプレート] に移動します。

2. [インポート] をクリックしてから、テンプレートが保存された.dat ファイルを選択します。

3. [開く] をクリックします。

   インポートが成功したかどうかを示すメッセージが表示されます。インポートするテンプレートがすでに存在する場合は省略されます。

4. [すべてのエージェントに適用] をクリックします。

情報漏えい対策チャネル

ユーザは、さまざまなチャネルを通して機密情報を転送できます。Apex One は、次のチャネルを監視できます。

- ネットワークチャネル: 機密情報は、HTTP や FTP などのネットワークプロトコルを使用して転送されます。

- システムおよびアプリケーションチャネル: 機密情報は、エンドポイントのローカルアプリケーションや周辺機器を使用して転送されます。

ネットワークチャネル

情報漏えい対策は、次のネットワークチャネルを介したデータ転送を監視できます。

- メールクライアント
- FTP
- HTTP および HTTPS
- IM アプリケーション
- SMB プロトコル
- Web メール

監視するデータ転送を特定するには、情報漏えい対策でチェックする転送の範囲を設定する必要があります。選択した範囲に応じて、すべてのデータ転送を監視することも、ローカルエリアネットワーク (LAN) 外部の転送のみを監視することもできます。

転送範囲の詳細については、479 ページの「ネットワークチャネルの転送範囲と送信先」を参照してください。

メールクライアント

情報漏えい対策では、さまざまなメールクライアント経由で送信されるメールを監視します。また、データ識別子について、メールの件名、本文、および添付ファイルをチェックします。サポートしているメールクライアントの一覧については、次の Web サイトを参照してください。

https://success.trendmicro.com/jp/solution/1312344

監視は、ユーザがメールを送信しようとしたときに実行されます。メールにデータ識別子が含まれている場合は、情報漏えい対策によってそのメールが許可またはブロックされます。

監視対象外の内部メールドメインおよび監視対象のメールサブドメインを定義できます。

- 対象外のメールドメイン: 監視対象外ドメインに送信されるメールの転送は、ただちに許可されます。

  注意

  対象外のメールドメインへのデータ転送と、処理が「監視」に指定された監視対象のメールサブドメインへのデータ転送は、転送が許可される点で似ています。唯一の違いは、情報漏えい対策が対象外のメールドメインについて転送ログを記録しない点です。監視対象のメールサブドメインの場合、転送は常にログに記録されます。

- 監視対象のメールサブドメイン: 情報漏えい対策は、監視対象サブドメインへのメール転送を検出すると、ポリシーの処理をチェックします。この処理に応じて、転送が許可またはブロックされます。

  注意

  監視対象チャネルにメールクライアントを選択した場合、監視するメールはポリシーと一致する必要があります。一方、監視対象のメールサブドメインに送信されるメールは、ポリシーに一致しなくても自動的に監視されます。

ドメインは次の任意の形式を使用して指定します。複数のドメインはカンマで区切って入力してください。

- X400 形式。例: /O=Trend/OU=USA、/O=Trend/OU=China
- メールドメイン。例: `example.com`

SMTP プロトコルで送信されるメールメッセージの場合、送信先の SMTP サーバが次のリストに存在するかどうかがチェックされます。

1. 監視対象
2. 監視対象外

注意

監視対象および監視対象外の詳細については、490 ページの「監視対象外および監視対象の定義」を参照してください。

3. 対象外のメールドメイン
4. 監視対象のメールサブドメイン

これは、メールが監視対象のリストに含まれている SMTP サーバに送信される場合、そのメールが監視されることを意味します。SMTP サーバが監視対象のリストに含まれていない場合は、他のリストが確認されます。

他のプロトコルで送信されるメールの場合、次のリストのみが確認されます。

1. 対象外のメールドメイン
2. 監視対象のメールサブドメイン

FTP

FTP クライアントが、ファイルを FTP サーバにアップロードしようとしていることが検出されると、そのファイル内にデータ識別子が存在するか確認されます。この時点ではファイルはアップロードされていません。情報漏えい対策ポリシーに従って、Apex One はアップロードを許可またはブロックします。

ファイルアップロードをブロックするポリシーを設定する場合は、次の点を考慮してください。

- Apex One がアップロードをブロックすると、一部の FTP クライアントはファイルのアップロードを再試行します。この場合、Apex One は FTP クライアントを終了して、再アップロードを阻止します。FTP クライアントが強制終了されてもユーザに通知はありません。情報漏えい対策ポリシーを公開するときに、この状況をユーザに説明してください。
- アップロードするファイルによって FTP サーバのファイルが上書きされる場合、FTP サーバ上のファイルは削除される可能性があります。

サポートしている FTP クライアントの一覧については、情報漏えい対策オプションリストのドキュメントを参照してください。

https://success.trendmicro.com/jp/solution/1312344

HTTP および HTTPS

Apex One は、HTTP または HTTPS 経由で転送されるデータを監視します。HTTPS の場合、Apex One は、暗号化して転送される前のデータをチェックします。

サポートしている Web ブラウザおよびアプリケーションの一覧については、情報漏えい対策オプションリストのドキュメントを参照してください。

https://success.trendmicro.com/jp/solution/1312344

IM アプリケーション

Apex One は、インスタントメッセージング (IM) アプリケーション経由で送信されるメッセージとファイルを監視します。ユーザが受信するメッセージとファイルは監視されません。

サポートしている IM アプリケーションの一覧については、情報漏えい対策オプションリストのドキュメントを参照してください。

https://success.trendmicro.com/jp/solution/1312344

Apex One は、AOL Instant Messenger、MSN、Windows Messenger、または Windows Live Messenger 経由で送信されるメッセージまたはファイルをブロックすると同時に、アプリケーション自体も終了します。Apex One によって終了されなかった場合も、アプリケーションは応答しなくなるため、結果的にユーザがアプリケーションを終了することになります。アプリケーションが強制終了されてもユーザに通知はありません。情報漏えい対策ポリシーを公開するときに、この状況をユーザに説明してください。

SMB プロトコル

Apex One は、共有ファイルアクセスを実現するサーバメッセージブロック (SMB) プロトコル経由のデータ転送を監視します。あるユーザの共有ファイルを他のユーザがコピーまたは読み取ろうとすると、Apex One によって、そのファイルがデータ識別子であるか、またはデータ識別子を含んでいるかが確認され、次にその操作が許可またはブロックされます。

注意

デバイスコントロール処理は情報漏えい対策処理よりも優先されます。たとえば、マップされたネットワークドライブでのファイルの移動がデバイスコントロールで許可されない場合は、情報漏えい対策で許可されても機密データの転送は開始されません。

デバイスコントロール処理の詳細については、434 ページの「ストレージデバイスに対する権限」を参照してください。

Apex One が共有ファイルアクセスを監視するアプリケーションの一覧については、情報漏えい対策オプションリストのドキュメントを参照してください。

https://success.trendmicro.com/jp/solution/1312344

Web メール

Web ベースのメールサービスは HTTP 経由でデータを転送します。Apex One はサポートされているサービスからの発信データを検出すると、そのデータ内にデータ識別子が存在するかどうかを確認します。

サポートしている Web ベースメールサービスの一覧については、情報漏えい対策オプションリストのドキュメントを参照してください。

https://success.trendmicro.com/jp/solution/1312344

ネットワークチャネルの転送範囲と送信先

情報漏えい対策で監視する必要のあるネットワークチャネルを介したデータ転送は、その転送範囲と送信先によって定義します。監視を必要とする転送では、転送を許可またはブロックする前に、データ識別子が存在するかどうかが確認されます。監視を必要としない転送では、データ識別子が存在するかどうかは確認されず、転送がただちに許可されます。

転送の範囲: すべての転送

情報漏えい対策では、ホストコンピュータから外部へ転送されるデータを監視します。

注意

外部エージェントにはこのオプションを選択することをお勧めします。

ホストコンピュータの外部にある特定の送信先へのデータ転送を監視しないようにするには、次の項目を定義します。

- 監視対象外: この送信先に転送されるデータは監視されません。

  注意

  監視対象外へのデータ転送と、処理が「監視」に指定された監視対象へのデータ転送は、転送が許可される点で似ています。唯一の違いは、情報漏えい対策が監視対象外について転送ログを記録しない点です。監視対象の場合、転送は常にログに記録されます。

- 監視対象: 監視対象外の中で監視を必要とする特別な送信先です。この送信先の指定には、次の制限があります。
  - 監視対象外を定義した場合のオプションです。
  - 監視対象外を定義していない場合には設定できません。

例:

次の IP アドレスが会社の法務部に割り当てられているとします。

- `10.201.168.1〜10.201.168.25`

現在、法務部の常勤社員を除く、全従業員の在籍証明書の転送を監視するポリシーを作成しています。この作業では、転送範囲として [すべての転送] を選択し、さらに次のいずれかを設定できます。

オプション	手順
オプション 1	1. 監視対象外に `10.201.168.1〜10.201.168.25` を追加します。 2. 法務部の非常勤社員の IP アドレスを監視対象に追加します。この IP アドレスは、`10.201.168.21〜10.201.168.23` の 3 つと仮定します。

オプション	手順
オプション 2	法務部の常勤社員の IP アドレスを監視対象外に追加します。 • 10.201.168.1-10.201.168.20 • 10.201.168.24-10.201.168.25

監視対象および監視対象外の定義方法のガイドラインについては、490 ページの「監視対象外および監視対象の定義」を参照してください。

転送の範囲: ローカルエリアネットワークの外部への転送のみ

情報漏えい対策では、ローカルエリアネットワーク (LAN) 外の送信先へ転送されるデータを監視します。

注意

内部エージェントにはこのオプションを選択することをお勧めします。

「ネットワーク」は、会社またはローカルのネットワークを指します。これには、現在のネットワーク (エンドポイントおよびネットマスクの IP アドレス) および次の標準のプライベート IP アドレスが含まれます。

- クラス A: 10.0.0.0〜10.255.255.255
- クラス B: 172.16.0.0〜172.31.255.255
- クラス C: 192.168.0.0〜192.168.255.255

この転送範囲を選択した場合、次のように定義できます。

- 監視対象外: 安全と考えられ、監視を必要としない LAN 外部の送信先を定義します。

  注意

  監視対象外へのデータ転送と、処理が「監視」に指定された監視対象へのデータ転送は、転送が許可される点で似ています。唯一の違いは、情報漏えい対策が監視対象外について転送ログを記録しない点です。監視対象の場合、転送は常にログに記録されます。

- 監視対象: LAN 内部の監視を必要とする送信先を定義します。

監視対象および監視対象外の定義方法のガイドラインについては、490 ページの「監視対象外および監視対象の定義」を参照してください。

競合の解決

転送範囲、監視対象、および監視対象外が競合する場合、Apex One では次の優先順位に従って認識が行われます。

- 監視対象
- 監視対象外
- 転送範囲

システムチャネルとアプリケーションチャネル

情報漏えい対策は、次のシステムおよびアプリケーションチャネルを監視できます。

- クラウドストレージサービス
- CD/DVD
- ピアツーピアアプリケーション
- PGP 暗号化
- プリンタ
- リムーバブルストレージ
- 同期ソフトウェア (ActiveSync)
- Windows クリップボード

クラウドストレージサービス

Apex One は、クラウドストレージサービスを使用してユーザがアクセスするファイルを監視します。サポートしているクラウドストレージサービスの一

覧については、情報漏えい対策オプションリストのドキュメントを参照してください。

https://success.trendmicro.com/jp/solution/1312344

CD/DVD

Apex One は、CD または DVD に記録されたデータを監視します。サポートしているデータ記録デバイスおよびソフトウェアの一覧については、情報漏えい対策オプションリストのドキュメントを参照してください。

https://success.trendmicro.com/jp/solution/1312344

サポートしているデバイス/ソフトウェアのいずれかで「作成」コマンドの実行が検出され、その処理が「放置 (ログのみ)」である場合、データの記録が続行されます。処理が「ブロック」の場合は、記録するどのファイルがデータ識別子であるか、またはデータ識別子を含んでいるか確認されます。Apex One が少なくとも 1 つデータ識別子を検出すると、すべてのファイル (データ識別子ではないファイルや、データ識別子を含むファイルもこれに含まれます) が記録されなくなります。Apex One では、CD または DVD の取り出しを防止することもできます。この問題が発生した場合、ソフトウェアプロセスの再起動か、デバイスのリセットを求めるメッセージが表示されます。

Apex One は、その他の CD/DVD 記録ルールも実装します。

- 誤検出を削減するために、Apex One は次のファイルを監視しません。

.bud	.dll	.gif	.gpd	.htm	.ico	.ini
.jpg	.lnk	.sys	.ttf	.url	.xml	

- Roxio データ記憶デバイスで使用される 2 つのファイルタイプ (*.png と *.skn) は性能を向上させるために監視されません。
- Apex One は次のディレクトリ内のファイルを監視しません。

*:¥autoexec.bat	*:¥Windows
..¥Application Data	..¥Cookies
..¥Local Settings	..¥ProgramData

```
..¥Program Files                    ..¥Users¥*¥AppData

..¥WINNT
```

- デバイスやソフトウェアで作成された ISO イメージは監視されません。

データ記憶デバイス (CD/DVD) へのアクセスのブロック

デバイスコントロールで制限できるのは、ライブファイルシステム形式を使用する CD/DVD 記憶デバイスへのアクセスだけです。マスター形式を使用する一部の他社製アプリケーションでは、デバイスコントロールを有効にしても引き続き読み取り/書き込み操作が可能な場合があります。フォーマットの種類に関係なく CD/DVD 記憶デバイスへのアクセスを制限するには、情報漏えい対策を使用します。

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [情報漏えい対策設定] の順にクリックします。
4. [外部エージェント] タブをクリックして外部エージェントのポリシーを設定するか、[内部エージェント] タブをクリックして内部エージェントのポリシーを設定します。

   注意

   エージェントの位置を設定していない場合は設定します。エージェントは、これらの位置設定を使用して、適用される正しい情報漏えい対策ポリシーを判断します。詳細については、640 ページの「エンドポイント (コンピュータ)の位置」を参照してください。

5. 次のいずれかを選択します。
   - [外部エージェント] タブで [内部エージェントにすべての設定を適用する] を選択すると、情報漏えい対策のすべての設定を内部エージェントに適用できます。

- [内部エージェント] タブで [外部エージェントにすべての設定を適用する] を選択すると、情報漏えい対策のすべての設定を外部エージェントに適用できます。

6. [ルール] タブで [追加] をクリックします。
7. [このルールを有効にする] を選択します。
8. ルールの名前を指定します。
9. [テンプレート] タブをクリックします。
10. リストから [すべてのファイル拡張子] テンプレートを選択して、[追加] をクリックします。
11. [チャネル] タブをクリックします。
12. [システムチャネルとアプリケーションチャネル] セクションで、[データ記憶デバイス (CD/DVD)] を選択します。
13. [処理] タブをクリックします。
14. [ブロック] 処理を選択します。
15. [保存]をクリックします。
16. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。

    - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
    - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

ピアツーピアアプリケーション

Apex One は、ピアツーピアアプリケーション経由で共有されているファイルを監視します。

サポートしているピアツーピアアプリケーションの一覧については、情報漏えい対策オプションリストのドキュメントを参照してください。

https://success.trendmicro.com/jp/solution/1312344

PGP 暗号化

Apex One は、PGP 暗号化ソフトウェアで暗号化されるデータを監視します。暗号化の開始前にデータがチェックされます。

サポートしている PGP 暗号化ソフトウェアの一覧については、情報漏えい対策オプションリストのドキュメントを参照してください。

https://success.trendmicro.com/jp/solution/1312344

プリンタ

Apex One は、さまざまなアプリケーションによって開始されたプリンタ操作を監視します。

保存前の新しいファイルに対するプリンタ操作は、その時点で印刷情報がメモリ上にしか存在しないためブロックされません。

プリンタ操作を開始可能なサポート対象アプリケーションの一覧については、情報漏えい対策オプションリストのドキュメントを参照してください。

https://success.trendmicro.com/jp/solution/1312344

リムーバブルストレージ

Apex One は、リムーバブルストレージデバイスへのデータ転送や、リムーバブルストレージデバイス内でのデータ転送を監視します。データ転送に関係する操作は次のとおりです。

- デバイス内部でのファイルの作成
- ホストコンピュータからデバイスへのファイルのコピー
- デバイス内部での変更されたファイルのクローズ
- デバイス内部でのファイル情報 (ファイルの拡張子など) の変更

転送されるファイルにデータ識別子が含まれている場合は、Apex One がその転送をブロックするか、許可します。

注意

- デバイスコントロール処理は情報漏えい対策処理よりも優先されます。たとえば、デバイスコントロールでリムーバブルストレージデバイスへのファイルのコピーが許可されない場合、情報漏えい対策で許可されても機密情報の転送は開始されません。

データ転送処理に利用可能なサポート対象のリムーバブルストレージデバイスおよびアプリケーションの一覧については、情報漏えい対策オプションリストのドキュメントを参照してください。

https://success.trendmicro.com/jp/solution/1312344

リムーバブルストレージデバイスへのファイル転送の処理は単純なプロセスです。たとえば、Microsoft Word でファイルを作成したユーザがそのファイルを SD カードに保存しようとしているとします (ユーザが保存するファイルタイプは問題ではありません)。そのファイルに転送が禁止されているデータ識別子が含まれている場合は、Apex One によってそのファイルの保存が阻止されます。

デバイス内部でのファイル転送の場合は、処理前に Apex One によってファイル (サイズが 75MB 以下の場合) が`%WINDIR%¥system32¥dgagent¥temp` にバックアップされます。ファイル転送が許可されると、バックアップファイルが削除されます。Apex One が転送をブロックした場合は、処理の過程でファイルが削除される可能性があります。この場合は、Apex One によって、オリジナルのファイルが存在したフォルダにバックアップファイルがコピーされます。

情報漏えい対策から除外するデバイスを定義できます。除外対象に指定したデバイスへのデータ転送や、デバイス内でのデータ転送は常に許可されます。

デバイスはそのベンダによって識別し、オプションで、デバイスのモデルやシリアル ID を指定します。

ヒント

デバイスリストツールは、エンドポイントに接続されたデバイスを照会する場合に使用します。このツールは、デバイスごとにデバイスのベンダ、モデル、およびシリアル ID を表示します。詳細については、443 ページの「デバイスリストツール」を参照してください。

同期ソフトウェア (ActiveSync)

Apex One は、同期ソフトウェア経由でモバイルデバイスに転送されるデータを監視します。

サポートしている同期ソフトウェアの一覧については、情報漏えい対策オプションリストのドキュメントを参照してください。

https://success.trendmicro.com/jp/solution/1312344

データの送信元 IP アドレスが 127.0.0.1 で、ポート 990 とポート 5678 のどちらか (同期に使用されるポート) を経由してそのデータが送信される場合、Apex One は、そのデータがデータ識別子かどうかをチェックしてから、その転送を許可またはブロックします。

Apex One がポート 990 上で転送されるファイルをブロックしたとき、モバイルデバイスの送信先フォルダに不正な形式の文字列を含む同じ名前のファイルが作成される場合があります。この現象は、Apex One が転送をブロックする前に、ファイルの一部がデバイスにコピーされたため発生します。

Windows クリップボード

Apex One は、Windows クリップボードに転送されるデータを監視して、その転送を許可またはブロックします。

また、ホストコンピュータと VMWare またはリモートデスクトップとのクリップボードの処理も監視できます。監視は、セキュリティエージェントがインストールされたエンティティで実行されます。たとえば、VMware 仮想マシンのセキュリティエージェントは、仮想マシンのクリップボードデータがホストコンピュータに転送されるのを阻止できます。同様に、セキュリ

ティエージェントがインストールされたホストコンピュータでは、リモートデスクトップ経由でアクセスするエンドポイントにクリップボードデータをコピーできません。

情報漏えい対策の処理

情報漏えい対策は、データ識別子の転送を検出すると、該当する情報漏えい対策ポリシーをチェックして、ポリシーに設定された処理を実行します。

次の表は、情報漏えい対策の処理をリストしたものです。

表 11-5. 情報漏えい対策の処理

処理	説明
処理	
放置	転送を許可し、ログに記録します。
ブロック	転送をブロックし、ログに記録します。
追加処理	
エージェントユーザに通知する	データの転送と、データがブロックされたかどうかを知らせる通知メッセージを表示します。
データを記録する	1 次処理に関係なく、機密情報を<セキュリティエージェントインストールフォルダ>¥DLPLite¥Forensic に記録します。情報漏えい対策によってフラグが付けられた機密情報を評価する場合にこの処理を選択します。 記録される機密情報は、ハードディスク容量を大量に消費する可能性があります。そのため、このオプションは機密性の高い情報に対してのみ有効にすることをお勧めします。
理由申請	「ブロック」処理を実行する前にユーザに確認メッセージを表示します。ユーザは、機密データを転送する理由を申請して「ブロック」処理を無効にできます。次のいずれかの理由を選択できます。 ・ この操作は確立された業務プロセスの一部です。 ・ このデータ転送は管理者から承認されています。

処理	説明
注意 このオプションは、[ブロック] 処理を選択した場合にのみ使用できます。	• このファイルには機密データは含まれません。 • その他: テキストフィールドに任意の理由を入力します。

情報漏えい対策の除外

情報漏えい対策の除外設定は、ポリシー内で定義されたすべてのルールを含め、ポリシー全体に適用されます。情報漏えい対策では、デジタル資産を検索する前に、すべての送信に除外設定を適用します。特定の送信がいずれかの除外ルールに一致すると、除外の種類に応じて、情報漏えい対策によって送信データがただちに許可または検索されます。

監視対象外および監視対象の定義

[チャネル] タブで設定された転送範囲に基づいて監視対象外および監視対象を定義します。[すべての転送] での監視対象外および監視対象の定義方法の詳細については、479 ページの「転送の範囲: すべての転送」を参照してください。[ローカルエリアネットワークの外部への転送のみ] での監視対象外および監視対象の定義方法の詳細については、481 ページの「転送の範囲: ローカルエリアネットワークの外部への転送のみ」を参照してください。

監視対象および監視対象外を定義する際は、次のガイドラインに従ってください。

1. 次の定義方法があります。
   - IP アドレス
   - ホスト名
   - FQDN
   - ネットワークアドレスとサブネットマスク (例: 10.1.1.1/32)

注意

サブネットマスクの場合、情報漏えい対策では CIDR (Classless Inter-Domain Routing) タイプのポートのみサポートされます。これは、255.255.255.0 の代わりに、32 のような数字のみ入力できることを意味します。

2. 特定のチャネルを送信先に指定する場合は、対象チャネルの初期設定のポート番号、または会社で定義されたポート番号を含めます。たとえば、ポート 21 は一般に FTP トラフィック用、ポート 80 は HTTP 用、およびポート 443 は HTTPS 用です。送信先とポート番号はコロンで区切ってください。

3. ポートの範囲を含めることもできます。すべてのポートを含めるには、ポート範囲は無視してください。

   送信先のポート番号とポート範囲の例を次に示します。

   - 10.1.1.1:80
   - host:5-20
   - host.domain.com:20
   - 10.1.1.1/32:20

4. 複数指定する場合はカンマで区切ります。

解凍ルール

圧縮ファイルに含まれるファイルを、デジタル資産について検索できます。情報漏えい対策は、次のルールを条件として、内部のファイルを検索する圧縮ファイルを決定します。

- 解凍ファイルのサイズが次の値を超える場合 — __ MB (1〜10240 MB)
- 圧縮階層数が次の値を超える場合 — __ (1-20)
- 検索対象ファイル数が次の値を超える場合 — __ (1-2000)

ルール 1:解凍後のファイルの最大サイズ

圧縮ファイルは、解凍後、指定された制限値を満たす必要があります。

例:制限を 20MB に設定したとします。

シナリオ 1:解凍後の archive.zip のサイズが 30MB になる場合、archive.zip に含まれるファイルはいずれも検索されません。他の 2 つのルールはそれ以降チェックされません。

シナリオ 2:解凍後の my_archive.zip のサイズが 10MB の場合は、次のように処理されます。

- my_archive.zip に圧縮ファイルが含まれていない場合、Apex One はルール 2 をスキップしてルール 3 を処理します。
- my_archive.zip に圧縮ファイルが含まれている場合、すべての圧縮後のファイルのサイズが制限値内である必要があります。たとえば、my_archive.zip に AAA.rar、BBB.zip および EEE.zip が含まれ、EEE.zip に 222.zip が含まれる場合、次のようになります。

```
my_archive.zip                    = 解凍後 10MB

        ¥AAA.rar                  = 解凍後 25MB

        ¥BBB.zip                  = 解凍後 3MB

        ¥EEE.zip                  = 解凍後 1MB

                ¥222.zip          = 解凍後 2MB
```

my_archive.zip、BBB.zip、EEE.zip、および 222.zip は、合計サイズが 20MB の制限内であるため、ルール 2 についてチェックされます。AAA.rar はスキップされます。

ルール 2:最大圧縮階層数

指定された階層数内のファイルに検索対象のフラグが付けられます。

次に例を示します。

```
my_archive.zip
                    ¥BBB.zip            ¥CCC.xls
                    ¥DDD.txt
                    ¥EEE.zip            ¥111.pdf
                                        ¥222.zip            ¥333.txt
```

階層数を 2 に制限を設定した場合:

- 333.txt は 3 番目の階層にあるため無視されます。
- 次のファイルに検索対象のフラグが付けられ、ルール 3 がチェックされます。
  - DDD.txt (最初の階層で検出)
  - CCC.xls (2 番目の階層で検出)
  - 111.pdf (2 番目の階層で検出)

ルール 3:検索するファイルの最大数

指定した最大数までファイルが検索されます。ファイルとフォルダは、数字、英文字の順番に検索されます。

ルール 2 の例では、太字のファイルに検索対象のフラグが付けられました。

```
my_archive.zip
                    ¥BBB.zip            ¥CCC.xls
                    ¥DDD.txt
                    ¥EEE.zip            ¥111.pdf
                                        ¥222.zip            ¥333.txt
```

さらに、my_archive.zip には、7Folder という名前のフォルダがあり、ルール 2 ではチェックされませんでした。このフォルダには FFF.doc および GGG.ppt が含まれています。この結果、検索されるファイルの合計数は、次の太字で示されている 5 ファイルになります。

```
my_archive.zip
                    ¥7Folder            ¥FFF.doc
                    ¥7Folder            ¥GGG.ppt
                    ¥BBB.zip            ¥CCC.xls
                    ¥DDD.txt
                    ¥EEE.zip            ¥111.pdf
                                        ¥222.zip            ¥333.txt
```

制限を 4 ファイルに設定した場合、次のファイルが検索されます。

- FFF.doc
- GGG.ppt
- CCC.xls
- DDD.txt

注意

組み込みファイルを含むファイルの場合は、その組み込みファイルの内容が展開されます。

展開された内容がテキストの場合、元のファイル (123.doc など) と組み込みファイル (abc.txt、xyz.xls など) は 1 つのファイルとしてカウントされます。

展開された内容がテキストではない場合、元のファイル (123.doc など) と組み込みファイル (abc.exe など) は別々にカウントされます。

解凍ルールが適用されるイベント

次のイベントの発生時に解凍ルールが適用されます。

表 11-6. 解凍ルールが適用されるイベント

転送される圧縮ファイルがポリシーと一致し、圧縮ファイルに対する処理が許可の場合 (ファイルが転送されます)。	たとえば、ユーザが転送する.ZIP ファイルを監視するには、ファイル属性 (ZIP) を定義してテンプレートに追加し、そのテンプレートをポリシーで使用します。そして、処理を「放置」に設定します。 **注意** 処理が「ブロック」の場合は、圧縮ファイル全体が転送されないため、内部のファイルを検索する必要はありません。
転送される圧縮ファイルがポリシーに一致しない場合。	Apex One では、この場合も圧縮ファイルに解凍ルールが適用され、どの内部ファイルをデジタル資産について検索する必要があるか、また圧縮ファイル全体を転送するかどうかが判定されます。

どちらのイベントも同じ結果になります。Apex One が圧縮ファイルを検出した場合の処理は、次のようになります。

- ルール 1 を満たさない場合、圧縮ファイル全体の転送が許可されます。
- ルール 1 を満たす場合、他の 2 つのルールがチェックされます。次の場合に圧縮ファイル全体の転送が許可されます。
  - 検索されたすべてのファイルがポリシーに一致しない場合
  - 検索されたすべてのファイルがポリシーに一致し、処理が「放置」である場合

    いずれかのファイルがポリシーに一致し、処理が「ブロック」の場合は、圧縮ファイル全体の転送がブロックされます。

情報漏えい対策のポリシー設定

データ識別子を設定し、それらをテンプレートで整理したら、情報漏えい対策ポリシーの作成に着手できます。

データ識別子とテンプレートに加えて、ポリシーの作成時にチャネルおよび処理を設定する必要があります。ポリシーの詳細については、453 ページの「情報漏えい対策のポリシー」を参照してください。

情報漏えい対策ポリシーの作成

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [情報漏えい対策設定] の順にクリックします。
4. [外部エージェント] タブをクリックして外部エージェントのポリシーを設定するか、[内部エージェント] タブをクリックして内部エージェントのポリシーを設定します。

   注意

   エージェントの位置を設定していない場合は設定します。エージェントは、これらの位置設定を使用して、適用される正しい情報漏えい対策ポリシーを判断します。詳細については、640 ページの「エンドポイント (コンピュータ)の位置」を参照してください。

5. [情報漏えい対策を有効にする] を選択します。
6. 次のいずれかを選択します。
   - [外部エージェント] タブで [内部エージェントにすべての設定を適用する] を選択すると、情報漏えい対策のすべての設定を内部エージェントに適用できます。

- [内部エージェント] タブで [外部エージェントにすべての設定を適用する] を選択すると、情報漏えい対策のすべての設定を外部エージェントに適用できます。

7. [ルール] タブで [追加] をクリックします。

   ポリシーに含めることのできるルールは最大 40 個です。

8. ルールの設定を行います。

   情報漏えい対策ルール作成の詳細については、497 ページの「情報漏えい対策ルールの作成」を参照してください。

9. [除外] タブをクリックし、必要な除外設定を行います。

   利用可能な除外設定の詳細については、490 ページの「情報漏えい対策の除外」を参照してください。

10. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。

    - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
    - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

情報漏えい対策ルールの作成

注意

情報漏えい対策は優先順位に従ってルールおよびテンプレートを処理します。ルールが「放置 (ログのみ)」に設定されている場合、情報漏えい対策はリスト内の次のルールを処理します。ルールが「ブロック」または「理由申請」に設定されている場合、情報漏えい対策はユーザ処理をブロックまたは承認し、そのルール/テンプレートをそれ以上処理しません。

手順

1. [このルールを有効にする] を選択します。
2. ルールの名前を指定します。

   ここからテンプレートの設定に移ります。
3. [テンプレート] タブをクリックします。
4. [利用可能なテンプレート] リストからテンプレートを選択して、[追加] をクリックします。

   テンプレートを選択する場合:

   - テンプレート名をクリックして名前を強調表示し、複数のエントリを選択します。
   - 検索機能は、特定のテンプレートを想定している場合に使用します。テンプレート名のすべてまたは一部を入力できます。

   注意

   ルールごとに最大 200 のテンプレートを含めることができます。
5. 目的のテンプレートが [利用可能なテンプレート] リストにない場合は、次の手順に従ってください。

   a. [新しいテンプレートの追加] をクリックします。

      [情報漏えい対策テンプレート] 画面が表示されます。

      [情報漏えい対策テンプレート] 画面でテンプレートを追加する手順については、469 ページの「情報漏えい対策テンプレート」を参照してください。

   b. テンプレートを作成したら、それを選択して [追加] をクリックします。

注意

テンプレートのチェックでは、最初に一致したルールが適用されます。つまり、あるテンプレートの定義にファイルまたはデータが一致した場合、他のテンプレートはチェックされません。優先度は、リストに表示されるテンプレートの順番に従います。

ここからチャネルの設定に移ります。

6. [チャネル] タブをクリックします。
7. ルールを適用するチャネルを選択します。

   チャネルの詳細については、475 ページの「ネットワークチャネル」、および 482 ページの「システムチャネルとアプリケーションチャネル」を参照してください。
8. いずれかのネットワークチャネルを選択した場合は、転送範囲を選択してください。
   - すべての転送
   - ローカルエリアネットワークの外部への転送のみ

   転送範囲の詳細、転送範囲に応じた送信先の振る舞い、および送信先を正しく定義する方法については、479 ページの「ネットワークチャネルの転送範囲と送信先」を参照してください。
9. [メールクライアント] を選択した場合は、次の手順に従ってください。
   a. [除外] をクリックします。
   b. 監視対象および監視対象外の内部メールドメインを指定します。

      監視対象および対象外のメールドメインの詳細については、475 ページの「メールクライアント」を参照してください。
10. [リムーバブルストレージ] を選択した場合は、次の手順に従ってください。
    a. [除外] をクリックします。
    b. ベンダで識別する監視対象外のリムーバブルストレージデバイスを追加します。デバイスモデルおよびシリアル ID は任意です。

USB デバイスの承認済みリストでは、アスタリスク (*) ワイルドカードを使用できます。任意のフィールドをアスタリスク (*) で置き換えると、他のフィールドを満たすデバイスをすべて含めることができます。

たとえば [ベンダ]-[モデル]-*は、シリアル ID に関係なく、指定したベンダの特定のモデルタイプのすべての USB デバイスを承認済みリストに配置します。

c. さらにデバイスを追加するには、プラス (+) アイコンをクリックします。

ヒント

デバイスリストツールは、エンドポイントに接続されたデバイスを照会する場合に使用します。このツールは、デバイスごとにデバイスのベンダ、モデル、およびシリアル ID を表示します。詳細については、443 ページの「デバイスリストツール」を参照してください。

ここから処理の設定に移ります。

11. [処理] タブをクリックします。
12. 1 次処理と追加処理を選択します。

    処理の詳細については、489 ページの「情報漏えい対策の処理」を参照してください。

13. [テンプレート]、[チャネル]、および[処理] の設定後、[保存] をクリックします。

情報漏えい対策ルールのインポート、エクスポート、およびコピー

管理者は、前に定義したルール (正しくフォーマットされた.dat ファイルに格納) をインポートしたり、情報漏えい対策ルールのリストをエクスポートしたりできます。情報漏えい対策ルールをコピーすると、管理者は前に定義したルールの内容を修正できるため、時間を節約できます。

次の表は各機能の動作について説明しています。

表 11-7. 情報漏えい対策ルールのインポート、エクスポート、およびコピーの機能

機能	説明
インポート	ルールリストをインポートすると、新しいルールが既存の情報漏えい対策ルールのリストに追加されます。情報漏えい対策は、対象リストにすでに存在するルールはスキップします。情報漏えい対策では、各ルールの事前設定はステータスの有効/無効を含めてすべて保持されます。
エクスポート	ルールリストをエクスポートすると、リスト全体が.dat ファイルにエクスポートされ、管理者はこのファイルを他のドメインやエージェントにインポートまたは配信できます。情報漏えい対策では、ルール設定はすべて現在の設定に基づいて保存されます。 注意 ・ 管理者は、リストをエクスポートする前に新しいまたは変更されたルールを保存または適用する必要があります。 ・ 情報漏えい対策は、各ルールの設定のみをエクスポートし、ポリシーの除外設定はエクスポートしません。
コピー	ルールをコピーすると、ルールの現在の設定の正確な複製が作成されます。管理者は、ルールの新しい名前を入力し、必要に応じて新しいルールの設定を変更することができます。

情報漏えい対策通知

Apex One には、Apex One 管理者やエージェントユーザにデジタル資産の転送について通知する初期設定のメッセージが用意されています。

管理者に送信される通知の詳細については、501 ページの「管理者向けの情報漏えい対策通知」を参照してください。

エージェントユーザに送信される通知の詳細については、505 ページの「エージェントユーザ向けの情報漏えい対策通知」を参照してください。

管理者向けの情報漏えい対策通知

デジタル資産の転送が検出されたとき、または転送がブロックされたときにだけ、管理者に通知を送信するように、Apex One を設定します。

Apex One には、管理者にデジタル資産の転送について通知する初期設定のメッセージが用意されています。これらの通知は、要件に合わせて変更したり、追加の通知を設定できます。

注意

Apex One は、メール、SNMP トラップ、および Windows NT イベントログで通知を送信できます。Apex One からこれらのチャネル経由で通知を送信するタイミングを設定します。詳細については、612 ページの「管理者通知設定」を参照してください。

管理者向けの情報漏えい対策通知の設定

手順

1. [管理] > [通知] > [管理者] に移動します。
2. [条件] タブで次の操作を実行します。
   a. [デジタル資産の転送] セクションに移動します。
   b. デジタル資産の転送が検出されたときに通知を送信するか (処理はブロックと許可のいずれか)、転送がブロックされた場合にのみ通知を送信するかを指定します。
3. [メール] タブで次の操作を実行します。
   a. [デジタル資産の転送] セクションに移動します。
   b. [メールによる通知を有効にする] を選択します。
   c. [エージェントツリーのドメイン権限を持つユーザに通知を送信する] を選択します。

      役割ベースの管理を使用して、エージェントツリーのドメイン権限をユーザに付与します。特定のドメインに属するエージェントで転送が検出されると、ドメイン権限を持つユーザのメールアドレスにメールが送信されます。次の表の例を参照してください。

表 11-8. エージェントツリードメインと権限

エージェントツリードメイン	ドメイン権限を持つ役割	役割を持つユーザアカウント	ユーザアカウントのメールアドレス
ドメイン A	管理者 (ビルトイン)	root	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
ドメイン B	管理者 (ビルトイン)	root	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

ドメイン A に属しているセキュリティエージェントがデジタル資産の転送を検出すると、mary@xyz.com、john@xyz.com、および chris@xyz.com にメールが送信されます。

ドメイン B に属しているセキュリティエージェントが転送を検出すると、mary@xyz.com と jane@xyz.com にメールが送信されます。

注意

このオプションを有効にする場合は、ドメイン権限を持つすべてのユーザが、対応するメールアドレスを持っている必要があります。メールアドレスを持たないユーザにはメール通知は送信されません。ユーザとメールアドレスは、[管理] > [アカウント管理] > [ユーザアカウント] で設定します。

d. [次のメールアドレスに通知メッセージを送信する] を選択し、メールアドレスを入力します。

e. 初期設定の件名とメッセージをそのまま使用するか変更します。[件名] および [メッセージ] では、トークン変数を使用してデータを表現できます。

表 11-9. 情報漏えい対策通知のトークン変数

変数	説明
%USER%	転送が検出されたときにエンドポイントにログオンしていたユーザ
%COMPUTER%	転送が検出されたエンドポイント
%DOMAIN%	エンドポイントのドメイン
%DATETIME%	転送が検出された日時
%CHANNEL%	転送が検出されたチャネル
%TEMPLATE%	検出を実行したデジタル資産のテンプレート
%RULE%	検出を実行したルール名 **注意** メッセージにルール名を表示するには、この変数を [メッセージ] に追加します。

4. [SNMP トラップ] タブで次の操作を実行します。
   a. [デジタル資産の転送] セクションに移動します。
   b. [SNMP トラップによる通知を有効にする] を選択します。
   c. 初期設定のメッセージをそのまま使用するか変更します。[メッセージ] では、トークン変数を使用してデータを表現できます。詳細については、504 ページの表 11-9 : 情報漏えい対策通知のトークン変数を参照してください。
5. [Windows イベントログ] タブで次の操作を実行します。
   a. [デジタル資産の転送] セクションに移動します。
   b. [Windows イベントログによる通知を有効にする] を選択します。
   c. 初期設定のメッセージをそのまま使用するか変更します。[メッセージ] では、トークン変数を使用してデータを表現できます。詳細については、504 ページの表 11-9 : 情報漏えい対策通知のトークン変数を参照してください。

6. [保存]をクリックします。

エージェントユーザ向けの情報漏えい対策通知

Apex One では、デジタル資産の転送が許可またはブロックされた直後にエージェントコンピュータに通知メッセージを表示できます。

デジタル資産の転送がブロックまたは許可されたことをユーザに通知するには、情報漏えい対策ポリシーを作成するときにオプションの [エージェントユーザに通知する] を選択します。ポリシーの作成手順については、496 ページの「情報漏えい対策のポリシー設定」を参照してください。

エージェント向けの情報漏えい対策通知の設定

手順

1. [管理] > [通知] > [エージェント] に移動します。
2. [種類] ドロップダウンで、[デジタル資産の転送] を選択します。
3. 初期設定のメッセージをそのまま使用するか変更します。
4. [保存]をクリックします。

情報漏えい対策ログ

エージェントはデジタル資産の転送 (ブロックおよび許可された転送) をログに記録し、そのログをサーバにただちに送信します。エージェントがログを送信できなかった場合は、5 分後に再試行します。

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログの削除スケジュールを設定します。ログの管理方法の詳細については、616 ページの「ログ管理」を参照してください。

情報漏えい対策ログの表示

手順

1. [エージェント] > [エージェント管理] または [ログ] > [エージェント] > [セキュリティリスク] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [ログ] > [情報漏えい対策ログ] または [ログの表示] > [情報漏えい対策ログ] をクリックします。
4. ログの条件を指定して [ログを表示する] をクリックします。
5. ログが表示されます。

   ログには、次の情報が含まれています。

表 11-10. 情報漏えい対策ログ情報

列	説明
日時	情報漏えい対策がイベントのログを記録した日付と時刻
ユーザ名	エンドポイントにログオンしていたユーザの名前
エンドポイント	情報漏えい対策が転送を検出したエンドポイントの名前
ドメイン	エンドポイントのドメイン
IP アドレス	エンドポイントの IP アドレス
ルール名	インシデントをトリガしたルール名 **注意** 前のバージョンのウイルスバスター Corp.で作成したポリシーには、LEGACY_DLP_Policy という初期設定の名前が表示されます。
チャネル	転送が発生したチャネル

列	説明
プロセス	デジタル資産の転送に利用されたプロセス (このプロセスはチャネルによって異なります) 詳細については、507 ページの「チャネルごとのプロセス」を参照してください。
ソース	デジタル資産を含むファイルの送信元、またはチャネル (送信元がない場合)
対象	デジタル資産が含まれているファイルの送信先、またはチャネル (送信元がない場合)
処理	転送に対する処理
ファイル/データサイズ	検出されたオブジェクトのサイズ
詳細	転送に関するその他の詳細情報を含むリンク 詳細については、510 ページの「情報漏えい対策ログの詳細」を参照してください。

6. ログを CSV ファイルに保存するには、[CSV 形式ですべてエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。

チャネルごとのプロセス

次の表に、情報漏えい対策ログの [プロセス] 列に表示されるプロセスを示します。

表 11-11. チャネルごとのプロセス

チャネル	プロセス
同期ソフトウェア (ActiveSync)	同期ソフトウェアのフルパスとプロセス名 例: `C:¥Windows¥system32¥WUDFHost.exe`

チャネル	プロセス
データレコーダー (CD/DVD)	データ記憶デバイスのフルパスとプロセス名 例: `C:¥Windows¥Explorer.exe`
Windows クリップボード	該当なし
メールクライアント - Lotus Notes	Lotus Notes のフルパスとプロセス名 例: `C:¥Program Files¥IBM¥Lotus¥Notes¥nlnotes.exe`
メールクライアント - Microsoft Outlook	Microsoft Outlook のフルパスとプロセス名 例: `C:¥Program Files¥Microsoft Office¥Office12¥OUTLOOK.EXE`
メールクライアント - SMTP プロトコルを使用するすべてのクライアント	メールクライアントのフルパスとプロセス名 例: `C:¥Program Files¥Mozilla Thunderbird¥thunderbird.exe`
リムーバブルストレージ	ストレージデバイスにデータを転送したアプリケーション、またはストレージデバイス内でデータを転送したアプリケーションのプロセス名 例: `explorer.exe`
FTP	FTP クライアントのフルパスとプロセス名 例: `D:¥Program Files¥FileZilla FTP Client¥filezilla.exe`
HTTP	[HTTP アプリケーション]
HTTPS	ブラウザまたはアプリケーションのフルパスとプロセス名 例: `C:¥Program Files¥Internet Explorer¥iexplore.exe`

チャネル	プロセス
IM アプリケーション	IM アプリケーションのフルパスとプロセス名 例: C:¥Program Files¥Skype¥Phone¥Skype.exe
IM アプリケーション - MSN	• MSN のフルパスとプロセス名 例: C:¥Program Files¥Windows Live¥Messenger¥msnmsgr.exe • [HTTP アプリケーション] (データがチャット画面から転送された場合)
ピアツーピアアプリケーション	ピアツーピアアプリケーションのフルパスとプロセス名 例: D:¥Program Files¥BitTorrent¥bittorrent.exe
PGP 暗号化	PGP 暗号化ソフトウェアのフルパスとプロセス名 例: C:¥Program Files¥PGP Corporation¥PGP Desktop¥PGPmnApp.exe
プリンタ	プリンタ操作を開始したアプリケーションのフルパスとプロセス名 例: C:¥Program Files¥Microsoft Office¥Office12¥ WINWORD.EXE
SMB プロトコル	共有ファイルアクセス (新しいファイルのコピーまたは作成) を実行したアプリケーションのフルパスとプロセス名 例: C:¥Windows¥Explorer.exe
Web メール (HTTP モード)	[HTTP アプリケーション]

チャネル	プロセス
Web メール (HTTPS モード)	ブラウザまたはアプリケーションのフルパスとプロセス名 例: C:¥Program Files¥Mozilla Firefox¥firefox.exe

情報漏えい対策ログの詳細

[情報漏えい対策ログの詳細] 画面には、デジタル資産の転送に関するその他の詳細情報が表示されます。転送の詳細情報は、Apex One がイベントを検出したチャネルやプロセスによって異なります。

次の表に、表示される詳細情報について示します。

表 11-12. 情報漏えい対策ログの詳細

詳細	説明
日時	情報漏えい対策がイベントのログを記録した日付と時刻
違反 ID	イベントの一意の ID
ユーザ名	エンドポイントにログオンしていたユーザの名前
エンドポイント	情報漏えい対策が転送を検出したエンドポイントの名前
ドメイン	エンドポイントのドメイン
IP アドレス	エンドポイントの IP アドレス
チャネル	転送が発生したチャネル
プロセス	デジタル資産の転送に利用されたプロセス (このプロセスはチャネルによって異なります) 詳細については、507 ページの「チャネルごとのプロセス」を参照してください。
ソース	デジタル資産を含むファイルの送信元、またはチャネル (送信元がない場合)
メール送信者	転送の発生源となったメールアドレス

詳細	説明
メールの件名	デジタル資産を含むメールメッセージの件名
メール受信者	メールメッセージの受信者のメールアドレス
URL	Web サイトまたは Web ページの URL
FTP ユーザ	FTP サーバへのログオンに使用されたユーザ名
ファイルクラス	情報漏えい対策がデジタル資産を検出したファイルの種類
ルール/テンプレート	実際に検出を実行したルール名およびテンプレートのリスト
処理	転送に対する処理
理由申請	機密データの転送を続行するためにユーザが申請した理由

情報漏えい対策オプションモジュールのデバッグログの有効化

手順

1. サポートセンターから `logger.cfg` ファイルを入手します。
2. `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite` (32 ビット版システムの場合) または `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\DlpLite` (64 ビット版システムの場合) に次のデータを追加します。
   - 種類: `String`
   - 名前: `debugcfg`
   - 値: `C:¥Log¥logger.cfg`
3. `C:¥`ディレクトリに、「Log」という名前のフォルダを作成します。
4. `Log` フォルダに「logger.cfg」をコピーします。
5. Web コンソールから情報漏えい対策とデバイスコントロールの設定を配信して、ログの収集を開始します。

注意

情報漏えい対策オプションモジュールのデバッグログを無効にするには、レジストリキーの `debugcfg` を削除し、エンドポイントを再起動します。

第 12 章

Web レピュテーションの使用

この章では、Web ベースの脅威と、Apex One を使用してネットワークやコンピュータを Web ベースの脅威から保護する方法について説明します。

この章は次のトピックで構成されます。

Web からの脅威について

Web からの脅威には、インターネットで発生する広範囲にわたる脅威が含まれます。Web からの脅威はその手法が巧妙化しており、単独のファイルや手法ではなく、さまざまなファイルやテクニックが併用されています。たとえば、Web からの脅威の作成者は、使用するバージョンや亜種を絶えず変えています。Web からの脅威は、感染したエンドポイント上ではなく Web サイトの一定の場所に存在するため、作成者は検出を逃れるために定期的にそのコードを変更しています。

かつて、ハッカー、ウイルスライター、スパムメール送信者、スパイウェア作成者と呼ばれていた人たちは、最近ではサイバー犯罪者と呼ばれるようになりました。Web からの脅威は、このような犯罪者が 2 つの目的のいずれかを達成するために利用されます。目的の 1 つは、今後の営業に関する情報を盗難することです。これにより、個人情報の損失という形で、機密情報の漏えいが発生します。また、感染したエンドポイントは、フィッシング攻撃やその他の情報収集活動を拡大するための媒介物として利用される場合もあります。さらに、この脅威によって、Web 商取引での信用を喪失し、インターネット取引に必要な信頼関係が崩壊してしまう危険性もあります。第 2 の目的は、ユーザの CPU の処理能力を奪い取って、金儲け活動の道具として利用することです。この活動には、分散型のサービス拒否攻撃やペイパークリック活動という形を取った、スパムメールの送信や支払いの強要などがあります。

C&C コンタクトアラートサービス

トレンドマイクロのコマンド&コントロール (C&C) コンタクトアラートサービスでは、検出およびアラート機能が向上し、APT (標的型サイバー攻撃)やターゲット攻撃によるダメージを軽減できます。C&C コンタクトアラートサービスは Web レピュテーションサービスと統合され、Web レピュテーションのセキュリティレベルに基づいて、検出されたコールバックアドレスに対して実行される処理を決定します。

また、C&C IP リストにより、ネットワークコンテンツ検査エンジンを使用した C&C コールバックの検出がさらに強化され、どのネットワークチャネルからでも C&C コンタクトを特定できます。

Web レピュテーションのセキュリティレベルの設定の詳細については、517 ページの「Web レピュテーションポリシーの設定」を参照してください。

表 12-1. C&C コンタクトアラートサービスの機能

機能	説明
グローバルインテリジェンスリスト	Trend Micro Smart Protection Network は、世界各地のソースからのグローバルインテリジェンスリストを集め、各 C&C コールバックアドレスのリスクレベルをテストし、評価します。Web レピュテーションサービスは、グローバルインテリジェンスリストを不正な Web サイトのレピュテーションスコアとともに使用し、高度な脅威に対するセキュリティを強化します。Web レピュテーションのセキュリティレベルにより、割り当てられたリスクレベルに基づいて不正な Web サイトや C&C サーバに対して実行される処理が決定されます。
仮想アナライザリスト	Smart Protection Server を仮想アナライザと統合して、仮想アナライザの C&C サーバリストを取得することができます。仮想アナライザは、ヒューリスティクスと行動に基づく高度なテスト方法を使用して、安全な環境における潜在的なリスクを評価し、分析した脅威にリスクレベルを割り当てます。仮想アナライザは、C&C サーバの可能性のあるサーバへの接続を試みた脅威を、仮想アナライザリストに入力します。仮想アナライザリストは企業固有のもので、ターゲット攻撃に対する防御をより高度にカスタマイズできます。 Apex One は、仮想アナライザからリストを取得し、グローバルインテリジェンスとローカル仮想アナライザリストの両方に照らしてすべての C&C 脅威を評価します。 仮想アナライザの不審オブジェクトリストの接続の詳細については、608 ページの「不審オブジェクトリストの設定」を参照してください。
不審接続監視サービス	不審接続監視サービスは、ユーザ指定およびグローバル IP C&C リストを管理し、エンドポイントから潜在的な C&C サーバへの接続の挙動を監視します。 詳細については、395 ページの「不審接続監視サービス」を参照してください。
管理者通知	管理者は、C&C コールバックが検出された後に、詳細でカスタマイズ可能な通知を受信するよう選択できます。 詳細については、526 ページの「管理者向けの C&C コールバック通知の設定」を参照してください。

機能	説明
エージェント通知	管理者は、エンドポイントで C&C コールバックが検出された後に、詳細でカスタマイズ可能な通知をエージェントユーザに送信するよう選択できます。 詳細については、529 ページの「エージェントユーザ向けの C&C コンタクトアラート通知」を参照してください。
アウトブレーク通知	管理者は、アウトブレーク通知を C&C コールバックイベントごとに固有にカスタマイズして、アウトブレークが 1 つのエンドポイントで発生したか、またはネットワーク全体で発生したかを指定できます。 詳細については、530 ページの「C&C コールバックアウトブレーク」を参照してください。
C&C コールバックログ	ログにより、すべての C&C コールバックイベントに関する詳細情報が提供されます。 詳細については、534 ページの「C&C コールバックログの表示」を参照してください。

Web レピュテーション

Web レピュテーションテクノロジは、Web サイトの経過日数、配置場所の変更履歴、および不正プログラムの挙動分析により検出された不審な活動の兆候などの要素に基づいてレピュテーションスコアを割り当てることにより、Web ドメインの信頼性を追跡します。トレンドマイクロでは、Web サイトを継続的に分析して Web レピュテーションスコアをアップデートし、不正と思われるコンテンツにユーザがアクセスできないようにしています。

ユーザが Web サイトにアクセスしようとすると、セキュリティエージェントは Smart Protection ソースに対するクエリを実行して、コンテンツのリスクレベルを特定します。Web サイトへのアクセスを許可するかどうかは、セキュリティエージェントに対して設定された Web レピュテーションポリシーによって決まります。

注意

Trend Micro Smart Protection ソースの詳細については、123 ページの「Trend Micro Smart Protection ソースリスト」を参照してください。

Web レピュテーションの機能を使用すると、安全または危険と見なされる Web サイトを承認済みリストまたはブロックリストに追加できます。セキュリティエージェントは、これらのリストに追加された Web サイトについて Web レピュテーションスコアを照会せず、アクセスを自動的に許可またはブロックします。

Web レピュテーションポリシー

Web レピュテーションポリシーによって、Apex One が Web サイトへのアクセスをブロックするか許可するかが決まります。

内部エージェントと外部エージェントに対してポリシーを設定できます。通常、Apex One 管理者は、外部エージェントに対してより厳格なポリシーを設定します。

ポリシーは、Apex One エージェントツリーで細かく設定されます。特定のポリシーを、エージェントグループに適用したり、個別のエージェントに適用したりできます。また、単一のポリシーをすべてのエージェントに適用することもできます。

ポリシーが配信されると、エージェントは エンドポイントの位置 画面 (640 ページの「エンドポイント (コンピュータ)の位置」を参照) で設定された位置の基準を使用して、その位置と適用されるポリシーを判断します。エージェントのポリシーは、位置が変わるたびに切り替えられます。

Web レピュテーションポリシーの設定

組織の HTTP 通信を処理するプロキシサーバを設定しており、Web アクセスを許可する前に認証を要求する場合は、プロキシサーバ認証の資格情報を指定します。

詳細については、690 ページの「外部エージェントのプロキシ設定」を参照してください。

手順

1. [エージェント] > [エージェント管理]に移動します。

2. エージェントツリーで対象を選択します。
3. [設定] > [Web レピュテーション設定] をクリックします。
4. [外部エージェント] タブを選択して外部エージェントのポリシーを設定するか、[内部エージェント] タブを選択して内部エージェントのポリシーを設定します。

ヒント

エージェントの位置を設定していない場合は設定します。この設定をもとにエンドポイントの位置が判断され、正しい Web レピュテーションポリシーが適用されます。詳細については、640 ページの「エンドポイント (コンピュータ)の位置」を参照してください。

---

5. [次の OS で Web レピュテーションを有効にする] で、保護する Windows プラットフォームの種類 ([Windows デスクトッププラットフォーム] および [Windows Server プラットフォーム]) を選択します。

ヒント

Web レピュテーション機能を備えたトレンドマイクロ製品 (Trend Micro InterScan Web Security Virtual Appliance など) をすでに使用している場合には、内部エージェントの Web レピュテーションは無効にすることをお勧めします。

Web レピュテーションポリシーを有効にした場合は次のように動作します。

- Web レピュテーションクエリをローカルの Smart Protection Server に送信するよう、内部のオンプレミスセキュリティエージェントを設定するだけです。
- 内部エージェントは、次の Web レピュテーションソースに Web レピュテーションクエリを送信します。
  - [Smart Protection Server にクエリを送信する] オプションが有効な場合には Smart Protection Server に送信します。
  - [Smart Protection Server にクエリを送信する] オプションが無効な場合には Trend Micro Smart Protection Network に送信します。

6. [HTTPS URL を確認する] を選択します。

重要

HTTPS URL の検索では、HTTP/2 プロトコルもサポートされます。Web レピュテーションで HTTPS URL または HTTP/2 URL を確認する前に、ブラウザごとにいくつかの設定を済ませておく必要があります。

詳細については、523 ページの「HTTPS URL 検索のサポート」を参照してください。

---

7. 内部セキュリティエージェントから Smart Protection Server に Web レピュテーションクエリを送信する場合は、[Smart Protection Server にクエリを送信する] を選択します。

   - このオプションを有効にする場合は、次の点に注意してください。
     - エージェントは、Trend Micro Smart Protection ソースリストを参照して、クエリを送信する Smart Protection Server を決定します。

       Smart Protection ソースリストの詳細については、123 ページの「Trend Micro Smart Protection ソースリスト」を参照してください。

     - Smart Protection Server が使用可能であることを確認します。どの Smart Protection Server も使用できない場合、エージェントは Smart Protection Network にクエリを送信しません。この場合、エージェントが使用できる Web レピュテーションデータソースは承認済み URL リスト/URL ブロックリストのみです。
     - エージェントからプロキシサーバ経由で Smart Protection Server に接続する必要がある場合は、[管理] > [設定] > [プロキシ] > [エージェント] タブの [内部プロキシ] でプロキシ設定を指定します。
     - Smart Protection Server を定期的に更新して、保護を最新の状態に維持してください。
     - 評価されていない Web サイトはブロックされません。これらの Web サイトの Web レピュテーションデータは Smart Protection Server で保存されません。

- このオプションを無効にする場合は、次の点に注意してください。
  - エージェントは、Trend Micro Smart Protection Network に Web レピュテーションクエリを送信します。クエリを送信するために、エンドポイントにはインターネット接続が必要です。
  - Trend Micro Smart Protection Network への接続にプロキシサーバ認証が必要な場合は、[管理] > [設定] > [プロキシ] > [エージェント] タブ > [外部プロキシ] で認証アカウント情報を指定します。
  - [トレンドマイクロによってまだ評価されていないページをブロックする] オプションを選択した場合、評価されていない Web サイトがブロックされます。

8. Web レピュテーションセキュリティレベルを [高]、[中]、[低] から選択します。

注意

Web レピュテーションは、セキュリティレベルに従って URL へのアクセスを許可するかブロックするかを決定します。たとえば、セキュリティレベルを低に設定すると、Web レピュテーションは Web からの脅威と認識されている URL のみをブロックします。セキュリティレベルをより高く設定すると、Web からの脅威の検出率が増加しますが、誤検出の可能性も増加します。

---

9. [トレンドマイクロによってまだ評価されていないページをブロックします] は、[Smart Protection Server にクエリを送信する] オプションを無効にした場合に選択できます。

注意

トレンドマイクロは、安全のために Web ページを積極的に評価していますが、ユーザが新しい Web サイトやあまり利用されない Web サイトにアクセスすると、未評価のページに遭遇する可能性があります。未評価のページへのアクセスをブロックすると、安全性は向上しますが、安全なページへのアクセスもブロックされる場合があります。

---

10. Web ブラウザの脆弱性および不正なスクリプトを特定し、Web ブラウザをセキュリティ侵害から保護するには、[不正なスクリプトを含むページをブロックする] を選択します。

Web レピュテーションは、ブラウザ脆弱性対策パターンファイルとスクリプトアナライザパターンファイルの両方を利用して、システムが危険にさらされる前に Web ページを特定してブロックします。

重要

- ブラウザ脆弱性対策機能では、Internet Explorer、Microsoft Edge レガシ、Microsoft Edge Chromium、Mozilla Firefox、Chrome の各ブラウザがサポートされます。
- ブラウザ脆弱性対策機能を使用するには、高度な保護サービスを有効にする必要があります。

重要

ブラウザ脆弱性対策機能を使用するには、高度な保護サービスを有効にする必要があります。

高度な保護サービスを有効にするには、[エージェント] > [エージェント管理] に移動し、[設定] > [追加サービス設定] をクリックします。

セキュリティエージェントで初めてブラウザ脆弱性対策機能を有効にした場合は、ブラウザ脆弱性対策が機能するためには、ブラウザで必要なアドオンを有効にする必要があります。Internet Explorer 9、10、または 11 を実行するセキュリティエージェントの場合は、ブラウザのポップアップウィンドウで `Trend Micro IE Protection` アドオンを有効にする必要があります。

11. 承認済みリストとブロックリストを設定します。

注意

承認済みリストはブロックリストより優先されます。ある URL が承認済みリストのエントリに一致する場合は、同じ URL がブロックリストにあってもその URL へのアクセスは常に許可されます。

a. [承認済み/ブロックリストを有効にする] を選択します。

b. URL を入力します。

URL では、任意の場所でワイルドカード文字 (*) を使用できます。

例:

- 「www.trendmicro.com/*」と入力すると、トレンドマイクロの Web サイト内のすべてのページが Web レピュテーションで承認されます。
- 「*.trendmicro.com/*」と入力すると、trendmicro.com のサブドメインのすべてのページが Web レピュテーションで承認されます。

IP アドレスを含む URL も入力できます。URL が IPv6 アドレスを含む場合は、アドレスをカッコ () で囲んで指定します。

c. [承認済みリストに追加]、または [ブロックリストに追加] をクリックします。

d. リストを.dat ファイルにエクスポートするには、[エクスポート] をクリックし、[保存] をクリックします。

e. 別のサーバからリストをエクスポートしている場合、この画面にインポートするときは、[インポート] をクリックして、.dat ファイルを選択します。リストが画面にロードされます。

重要

Web レピュテーションは、承認済みリストとブロックリストにあるアドレスに対しては検索を実行しません。

---

12. Web レピュテーションのフィードバックを送信するには、[URL の再診断] にある URL をクリックします。ブラウザウィンドウに Trend Micro Site Safety Center が表示されます。

13. セキュリティエージェントからサーバへのレピュテーションログの送信を許可するかどうかを選択します。Web レピュテーションでブロックされている URL を分析して安全と考えられる URL に対して適切な処理を実行する場合には、エージェントからのログの送信を許可してください。

14. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。

- すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェン

トに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。

- 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

HTTPS URL 検索のサポート

HTTPS 通信では、証明書を使用して Web サーバを識別します。またデータを暗号化することで、漏えいや盗聴から情報を保護します。より安全な手法ですが、HTTPS を使用した Web サイトへのアクセスにも危険はあります。有効なセキュリティ証明書を使用していても、それが感染しているサイトであれば、不正プログラムがホストされていたり個人情報が盗まれる可能性があります。証明書は比較的容易に入手できるため、HTTPS を使用する不正な Web サーバを簡単に設定することもできます。

重要

Windows 8.1 (以降)、および Windows Server 2012 (以降) においては、Internet Explorer の HTTPS 検索がデスクトップモードにのみ対応します。

[HTTPS URL を確認する] を有効にすると、HTTPS を使用する感染しているサイトや不正なサイトにアクセスする危険性を低減できます。Web レピュテーションでは、次のブラウザで HTTPS トラフィックを監視できます。

表 12-2. HTTPS トラフィックでサポートされるブラウザ

ブラウザ	バージョン番号	前提条件
Microsoft Internet Explorer	8.x	最新バージョン
	9.x	ブラウザのポップアップウィンドウで `Trend Micro Osprey Plugin Class` アドオンを有効にする必要があります。
	10.x	
	11.x	

ブラウザ	バージョン番号	前提条件
Mozilla Firefox	3.5 以降	なし
Chrome	最新バージョン	
Microsoft Edge	• レガシ • Chromium	

Web レピュテーション用に Internet Explorer を設定する方法の詳細については、次の製品 Q&A 記事を参照してください。

- https://success.trendmicro.com/jp/solution/1098874
- https://success.trendmicro.com/jp/solution/1111399

エージェントユーザ向けの Web からの脅威の通知

Apex One では、Web レピュテーションポリシーに違反する URL をブロックした直後に、セキュリティエージェントエンドポイントに通知メッセージを表示できます。通知メッセージを有効にして、必要に応じて通知メッセージの内容を修正してください。

Web からの脅威の通知メッセージの有効化

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [その他の設定] タブをクリックします。

5. [Web レピュテーション設定] セクションで、[Web サイトのブロック時に通知を表示] を選択します。
6. [C&C コンタクトアラート設定] セクションで、[C&C コールバックが検出された場合、通知を表示] を選択します。
7. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。
   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
   - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

Web からの脅威の通知の変更

手順

1. [管理] > [通知] > [エージェント] に移動します。
2. [種類] のドロップダウンから、変更する Web からの脅威の通知の種類を選択します。
   - Web レピュテーション違反
   - C&C コールバック
3. 表示されたテキストボックスで初期設定のメッセージを修正します。
4. [保存] をクリックします。

管理者向けの C&C コールバック通知

Apex One には、Apex One 管理者に C&C コールバックの検出について通知する初期設定の通知メッセージが用意されています。これらの通知は、要件に合わせて変更したり、追加の通知を設定できます。

管理者向けの C&C コールバック通知の設定

手順

1. [管理] > [通知] > [管理者] に移動します。
2. [条件] タブで次の操作を実行します。
   a. [C&C コールバック] セクションに移動します。
   b. Apex One が C&C コールバックを検出したときに通知を送信するか (処理のブロックまたはログへの記録が可能)、またはコールバックアドレスのリスクレベルが高の場合にのみ送信するかを指定します。
3. [メール] タブで次の操作を実行します。
   a. [C&C コールバック] セクションに移動します。
   b. [メールによる通知を有効にする] を選択します。
   c. [エージェントツリーのドメイン権限を持つユーザに通知を送信する] を選択します。

      役割ベースの管理を使用して、エージェントツリーのドメイン権限をユーザに付与します。特定のドメインに属するエージェントで転送が行われると、ドメイン権限を持つユーザのメールアドレスにメールが送信されます。次の表の例を参照してください。

表 12-3. エージェントツリードメインと権限

エージェントツリードメイン	ドメイン権限を持つ役割	役割を持つユーザアカウント	ユーザアカウントのメールアドレス
ドメイン A	管理者 (ビルトイン)	root	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
ドメイン B	管理者 (ビルトイン)	root	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

ドメイン A に属しているセキュリティエージェントが C&C コールバックを検出すると、mary@xyz.com、john@xyz.com、および chris@xyz.com にメールが送信されます。

ドメイン B に属しているセキュリティエージェントが C&C コールバックを検出すると、mary@xyz.com と jane@xyz.com にメールが送信されます。

注意

このオプションを有効にする場合は、ドメイン権限を持つすべてのユーザが、対応するメールアドレスを持っている必要があります。メールアドレスを持たないユーザにはメール通知は送信されません。ユーザとメールアドレスは、[管理] > [アカウント管理] > [ユーザアカウント] で設定します。

d. [次のメールアドレスに通知メッセージを送信する] を選択し、メールアドレスを入力します。

e. 初期設定の件名とメッセージをそのまま使用するか変更します。[件名] および [メッセージ] では、トークン変数を使用してデータを表現できます。

表 12-4. C&C コールバック通知のトークン変数

変数	説明
%CLIENTCOMPUTER%	コールバックを送信した対象エンドポイント
%IP%	対象エンドポイントの IP アドレス
%DOMAIN%	エンドポイントのドメイン
%DATETIME%	転送が検出された日時
%CALLBACKADDRESS%	C&C サーバのコールバックアドレス
%CNCRISKLEVEL%	C&C サーバのリスクレベル
%CNCLISTSOURCE%	C&C ソースリストの表示
%ACTION%	実行された処理

4. [SNMP トラップ] タブで次の操作を実行します。

   a. [C&C コールバック] セクションに移動します。

   b. [SNMP トラップによる通知を有効にする] を選択します。

   c. 初期設定のメッセージをそのまま使用するか変更します。[メッセージ] では、トークン変数を使用してデータを表現できます。詳細については、528 ページの表 12-4：C&C コールバック通知のトークン変数を参照してください。

5. [Windows イベントログ] タブで次の操作を実行します。

   a. [C&C コールバック] セクションに移動します。

   b. [Windows イベントログによる通知を有効にする] を選択します。

   c. 初期設定のメッセージをそのまま使用するか変更します。[メッセージ] では、トークン変数を使用してデータを表現できます。詳細については、528 ページの表 12-4：C&C コールバック通知のトークン変数を参照してください。

6. [保存] をクリックします。

エージェントユーザ向けの C&C コンタクトアラート通知

Apex One では、C&C サーバの URL をブロックした直後に、セキュリティエージェントコンピュータに通知メッセージを表示できます。通知メッセージを有効にして、必要に応じて通知メッセージの内容を修正してください。

C&C コールバック通知メッセージの有効化

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [その他の設定] タブをクリックします。
5. [C&C コンタクトアラート設定] セクションで、[C&C コールバックが検出された場合、通知を表示] を選択します。
6. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。
   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
   - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションで

は、既存のドメインに加えられる新しいエージェントには設定を適用しません。

C&C コールバック通知の変更

手順

1. [管理] > [通知] > [エージェント] に移動します。
2. [種類] のドロップダウンから、[C&C コールバック] を選択します。
3. 表示されたテキストボックスで初期設定のメッセージを修正します。
4. [保存] をクリックします。

C&C コールバックアウトブレーク

C&C コールバックアウトブレークをコールバックの数、送信元、およびリスクレベルによって定義します。

Apex One には、Apex One 管理者に大規模感染について通知する初期設定のメッセージが用意されています。通知メッセージは要求に合わせて変更できます。

注意

Apex One では、C&C コールバックアウトブレーク通知をメールで送信できます。Apex One から正常にメールが送信されるように、メールを設定します。詳細については、612 ページの「管理者通知設定」を参照してください。

C&C コールバックのアウトブレークの基準と通知の設定

手順

1. [管理] > [通知] > [アウトブレーク] に移動します。

   [アウトブレーク通知] 画面が表示されます。

2. [C&C コールバック] の [条件] タブで、次の項目を設定します。

オプション	説明
同様に感染しているホスト	エンドポイントごとにコールバック検出に基づいてアウトブレークを定義する場合に選択します。
C&C リスクレベル	アウトブレークが実行されるのは、すべての C&C コールバックか、または高リスクのソースのみかを指定します。
処理	大規模感染の状況を判断するために Apex One で考慮する必要のある処理を指定します。
検出数	大規模感染の状況を通知するために Apex One で必要な検出数を指定します。
期間	監視期間を指定します。

3. [メール] タブで次の操作を実行します。

   a. [C&C コールバック] で、[メールによる通知を有効にする] を選択します。

   b. [受信者] でメールの受信者を指定します。

   c. メール通知で使用する件名を [件名] に指定します。

   d. メッセージの内容を [メッセージ] に指定します。

      Apex One の [件名] と [メッセージ] では、トークンを使用できます。

      表 12-5. C&C コールバックアウトブレーク通知のトークン変数

変数トークン	説明
%C	C&C コールバックログの数

変数トークン	説明
%T	C&C コールバックログを累積する期間

e. 通知に含める追加のログデータを (表形式で) 指定します。

ログの列	説明
日時	検出の日時
感染ホスト	検出を含むエンドポイント
IP アドレス	感染ホストの IP アドレス
ドメイン	検出が行われたエンドポイントドメイン
コールバックアドレス	検出を実行した URL
C&C リスクレベル	コールバックアドレスのリスクレベル
C&C リストのソース	C&C サーバを特定した C&C リストのソース
処理	セキュリティリスクに対して実行された処理

4. [SNMP トラップ] タブで次の操作を実行します。
   a. [C&C コールバック] セクションに移動します。
   b. [SNMP トラップによる通知を有効にする] を選択します。
   c. 初期設定のメッセージをそのまま使用するか変更します。[メッセージ] では、トークン変数を使用してデータを表現できます。詳細については、531 ページの表 12-5：C&C コールバックアウトブレーク通知のトークン変数を参照してください。
5. [Windows イベントログ] タブで次の操作を実行します。
   a. [C&C コールバック] セクションに移動します。
   b. [Windows イベントログによる通知を有効にする] を選択します。
   c. 初期設定のメッセージをそのまま使用するか変更します。[メッセージ] では、トークン変数を使用してデータを表現できます。詳細につ

いては、531 ページの表 12-5：C&C コールバックアウトブレーク通知のトークン変数を参照してください。

6. [保存] をクリックします。

Web からの脅威のログ

サーバに Web レピュテーションログを送信するように、内部および外部エージェントの両方を設定します。Apex One にブロックされている URL を分析して、安全にアクセス可能と考えられる URL に対して適切な処理を実行する場合には、この設定を行います。

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログの削除スケジュールを設定します。ログの管理方法の詳細については、616 ページの「ログ管理」を参照してください。

Web レピュテーションログの表示

手順

1. 次のいずれかに移動します。
   - [ログ] > [エージェント] > [セキュリティリスク]
   - [エージェント] > [エージェント管理]
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [Web レピュテーションログ条件] 画面に移動します。
   - [セキュリティリスクログ] 画面で、[ログの表示] > [Web レピュテーションログ] の順にクリックします。
   - [エージェント管理] 画面で、[ログ] > [Web レピュテーションログ] の順にクリックします。

4. ログの条件を指定して [ログを表示する] をクリックします。
5. ログが表示されます。ログには、次の情報が含まれています。

項目	説明
日時	検出された日時
エンドポイント	検出が行われたエンドポイント
ドメイン	検出が行われたエンドポイントドメイン
URL	Web レピュテーションサービスによってブロックされた URL
リスクレベル	URL のリスクレベル
説明	セキュリティ上の脅威の説明
プロセス	接続が試行されたプロセス (path\application_name)
処理	検出に対して実行された処理

6. [承認済みリストに追加] をクリックして、ブロックしない URL を承認済み URL リストに追加します。
7. ログを CSV ファイルに保存するには、[CSV 形式ですべてエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。

C&C コールバックログの表示

手順

1. 次のいずれかに移動します。
   - [ログ] > [エージェント] > [セキュリティリスク]
   - [エージェント] > [エージェント管理]
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。

3. [C&C コールバックログ条件] 画面に移動します。
   - [セキュリティリスクログ] 画面で、[ログの表示] > [C&C コールバックログ] の順にクリックします。
   - [エージェント管理] 画面で、[ログ] > [C&C コールバックログ] の順にクリックします。
4. ログの条件を指定して [ログを表示する] をクリックします。
5. ログが表示されます。ログには、次の情報が含まれています。

項目	説明
日時	検出された日時
ユーザ	検出時にログオンしていたユーザ
感染ホスト	コールバックが発生したエンドポイント
IP アドレス	感染ホストの IP アドレス
ドメイン	検出が行われたエンドポイントドメイン
コールバックアドレス	エンドポイントからのコールバックの送信先となったアドレス
C&C リストのソース	C&C サーバを特定した C&C リストのソース
C&C リスクレベル	C&C サーバのリスクレベル
プロトコル	転送に使用されたインターネットプロトコル
プロセス	転送を開始したプロセス (path\application_name)
処理	検出に対して実行された処理

6. ブロックする必要のない URL が Web レピュテーションによってブロックされた場合は、[Web レピュテーション承認済みリストに追加] ボタンをクリックして、そのアドレスを Web レピュテーション承認済みリストに追加します。

注意

Web レピュテーション承認済みリストに追加できるのは URL だけです。グローバル C&C IP リストまたは仮想アナライザ (IP) C&C リストで検出された IP アドレスは、ユーザ指定の承認済み C&C IP リストに手動で追加してください。

詳細については、396 ページの「ユーザ指定の IP リストのグローバル設定」を参照してください。

7. ログを CSV ファイルに保存するには、[CSV 形式ですべてエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。

第 13 章

Apex One ファイアウォールの使用

この章では、Apex One ファイアウォールの機能と設定について説明します。

この章は次のトピックで構成されます。

Apex One ファイアウォールの概要

Apex One のファイアウォールは、ステートフルインスペクションおよび高性能なネットワークウイルス検索機能を使用して、ネットワーク上のセキュリティエージェントとサーバを保護します。Web ベースの管理コンソールで、接続をアプリケーション、IP アドレス、ポート番号、またはプロトコルに基づいてフィルタリングするルールを作成し、そのルールをさまざまなユーザグループに適用できます。

Apex One ファイアウォールに含まれる主要な機能および利点は次のとおりです。

トラフィックフィルタリング

Apex One のファイアウォールでは、次の条件に基づいて特定の種類のトラフィックをブロックする機能が用意されており、すべての送受信トラフィックをフィルタします。

- 方向 (受信/送信)
- プロトコル (TCP/UDP/ICMP/ICMPv6)
- 宛先ポート
- 送信元と送信先のエンドポイント

アプリケーションのフィルタ

Apex One のファイアウォールでは、ファイアウォールの除外リストで指定されたアプリケーションの受信および送信トラフィックをフィルタし、それらのアプリケーションがネットワークにアクセスすることを許可します。ネットワーク接続を使用できるかどうかは、管理者が設定したポリシーによって制御されます。

ソフトウェア安全性評価リスト

ローカルのソフトウェア安全性評価リストは、ファイアウォールポリシーのセキュリティレベルを回避できるアプリケーションのリストです。Apex One

のファイアウォールでは、ソフトウェア安全性評価リストで指定されたアプリケーションの実行およびネットワークへのアクセスを自動的に許可します。

また、トレンドマイクロのサーバでホストされる、動的に更新されたグローバルソフトウェア安全性評価リストのクエリをセキュリティエージェントに対して許可することもできます。

重要

グローバルソフトウェア安全性評価リストのクエリを実行するには、不正変更防止サービスとソフトウェア安全性評価サービスを有効にする必要があります。

ネットワークウイルスの検索

Apex One ファイアウォールでは、ネットワークウイルスに感染しているかどうかを判断するために各パケットを検査します。詳細については、272 ページの「ウイルスと不正プログラム」を参照してください。

カスタマイズ可能なプロファイルとポリシー

Apex One ファイアウォールには、指定したネットワークトラフィックをブロックまたは許可するためにポリシーを設定する機能があります。1 つまたは複数のプロファイルにポリシーを割り当てると、指定したセキュリティエージェントに配信できます。この機能では、エージェントのファイアウォール設定を高度にカスタマイズできます。

ステートフルインスペクション

Apex One のファイアウォールでは、ステートフルインスペクションを使用して、セキュリティエージェントへの接続を監視し、接続状態を記録します。接続における特定の状態の識別、後続動作の予測、および正常な接続が侵された場合の検出ができます。そのため、フィルタの判定は、プロファイルとポリシーのみを基準に実行されるのではなく、接続を分析し、ファイアウォールを通過したパケットをフィルタして確立したコンテキストも基準として実行されます。

ファイアウォール違反アウトブレークモニタ

Apex One ファイアウォールは、ファイアウォール違反が一定のしきい値を超えた特定の受信者に、カスタマイズした警告メッセージを送ります。しきい値を超えるということは、攻撃を受けていることを示す場合があります。

セキュリティエージェントファイアウォールの権限

セキュリティエージェントのコンソール上で、ファイアウォールの設定をセキュリティエージェントユーザに見せることができます。またユーザは、ファイアウォールおよびファイアウォール違反通知メッセージを有効/無効にすることができます。

Apex One ファイアウォールの有効化/無効化

Apex One サーバのインストール時には、Apex One ファイアウォールを有効にするか無効にするかを確認されます。

インストール時にファイアウォールを有効にし、特に Windows Server プラットフォームでパフォーマンスに影響が見られる場合には、ファイアウォールを無効にすることを検討してください。

インストール時にファイアウォールを無効にした後、エージェントを侵入から守るために有効にする場合は、まず 645 ページの「セキュリティエージェントサービス」のガイドラインと手順をお読みください。

すべてまたは選択したセキュリティエージェントエンドポイントでファイアウォールを有効または無効にすることができます。

Web コンソールで、次のいずれかの方法を使用してファイアウォールを有効または無効にします。

方法	手順
すべてのセキュリティエージェントで Apex One ファイアウォールを有効/無効にする	[グローバルエージェント設定] を使用して、すべてのセキュリティエージェントの Apex One ファイアウォールサービスを設定します。 詳細については、560 ページの「グローバルファイアウォール設定」を参照してください。 **注意** Apex One ファイアウォールを無効にすると、すべてのセキュリティエージェントのすべてのファイアウォールポリシーが自動的に無効になります。
Web コンソールからファイアウォールサービスを有効/無効にする	[追加サービス設定] を使用して、選択したセキュリティエージェントの Apex One ファイアウォールサービスを設定します。 詳細については、645 ページの「セキュリティエージェントサービス」を参照してください。 **注意** ファイアウォールサービスを無効にすると、選択したエージェントのすべてのファイアウォールポリシーが自動的に無効になります。
新しいポリシーを作成してセキュリティエージェントに適用する	1. ファイアウォールを有効/無効にする新しいポリシーを作成します。 新しいポリシーを作成する手順については、544 ページの「ファイアウォールポリシーの追加」を参照してください。 2. セキュリティエージェントにポリシーを適用します。

ファイアウォールポリシーおよびプロファイル

Apex One ファイアウォールでは、ポリシーおよびプロファイルを使用して、ネットワーク上のエンドポイントを保護する方法を構成し、カスタマイズできます。

Active Directory 統合と役割ベースの管理により、それぞれのユーザの役割では、権限に応じて、特定ドメインのポリシーやプロファイルを作成、設定、または削除できます。

ヒント

複数のベンダのファイアウォールを 1 つのエンドポイントにインストールすると、予期せぬ結果を招く恐れがあります。Apex One ファイアウォールを配信し有効にする前に、セキュリティエージェント上の異なるソフトウェアベースのファイアウォールアプリケーションを削除することを検討してください。

Apex One ファイアウォールを正常に使用するために必要な手順は次のとおりです。

1. ポリシーの作成。ポリシーによってセキュリティレベルを選択できます。セキュリティレベルに応じて、ネットワーク上のエンドポイントのトラフィックがブロックまたは許可され、ファイアウォール機能が有効になります。

2. 新規ポリシーを追加する場合、除外設定によって、ポリシーの除外をセキュリティエージェントに設定できます。ポリシーで全体的なブロックまたは許可のセキュリティレベルが設定されていても、エージェントに除外設定を指定すると、特定の種類のトラフィックを許可またはブロックできます。たとえば、ポリシーで一連のエージェントに対するすべてのトラフィックをブロックしても、HTTP トラフィックを許可する除外設定を作成すると、エージェントは Web サーバにアクセスできます。

3. プロファイルをセキュリティエージェントに作成し割り当てる場合ファイアウォールプロファイルは一連のエージェント属性を含みます。それぞれのプロファイルには参照しているポリシーが存在します。エージェントがプロファイル内に指定されている属性と一致した場合、関連ポリシーを起動します。

ファイアウォールポリシー

Apex One のファイアウォールポリシーを使用すると、ポリシーの除外設定で指定されていない特定の種類のネットワークトラフィックをブロックまたは許可することができます。また、ポリシーでは、Apex One ファイアウォール

のどの機能を有効または無効にするかを定義できます。1 つまたは複数のファイアウォールプロファイルにポリシーを割り当てます。

Active Directory 統合と役割ベースの管理により、それぞれのユーザの役割では、権限に応じて、特定ドメインのポリシーを作成、設定、または削除できます。

次の表に、ファイアウォールポリシーで使用できる設定を示します。

設定	説明
セキュリティレベル	セキュリティエージェントエンドポイントのすべての送受信トラフィックをブロックまたは許可する一般的な設定です。
ファイアウォール機能	Apex One ファイアウォールおよびファイアウォール違反通知メッセージの有効化/無効化を切り替えます。
ソフトウェア安全性評価リスト	安全と評価されたアプリケーションがネットワークに接続することを許可するかどうかを指定します。 詳細については、538 ページの「ソフトウェア安全性評価リスト」を参照してください。
ポリシー除外リスト	さまざまな種類のネットワークトラフィックをブロックまたは許可するために設定できる、除外設定のリストです。

注意

ファイアウォールプロファイルを作成するときに、セキュリティレベルやポリシー除外リストを変更する権限をエンドユーザに付与することができます。

詳細については、555 ページの「ファイアウォールプロファイルの追加」を参照してください。

初期設定のファイアウォールポリシー

Apex One には、一連の初期設定のポリシーが搭載されており、変更または削除することができます。

ポリシー名	セキュリティレベル	エージェント設定	除外	使用を推奨するケース
オールアクセスポリシー	低	ファイアウォールを有効にする	なし	エージェントにネットワークへの無制限のアクセスを許可するとき
Trend Micro Apex Central 用通信ポート	低	ファイアウォールを有効にする	ポート 80 および 10319 を経由するすべての受信/送信の TCP/UDP トラフィックを許可する	エージェントに MCP エージェントがインストールされているとき
InterScan for Microsoft Exchange コンソール	低	ファイアウォールを有効にする	ポート 16372 を経由するすべての受信/送信の TCP トラフィックを許可する	エージェントが InterScan for Microsoft Exchange コンソールにアクセスする必要があるとき
InterScan Messaging Security Suite コンソール	低	ファイアウォールを有効にする	ポート 80 を経由するすべての受信/送信の TCP トラフィックを許可する	エージェントが InterScan MSS コンソールにアクセスする必要があるとき

ファイアウォールポリシーの追加

手順

1. [エージェント] > [ファイアウォール] > [ポリシー] に移動します。
2. 新しいポリシーを追加するには、[追加] をクリックします。

   新しく作成するポリシーの設定が既存のポリシーの設定と類似する場合は、既存のポリシーを選択し、[コピー] をクリックします。
3. このポリシーの新しい名前を入力します。
4. セキュリティレベルを選択します。

   選択されたセキュリティレベルは、ファイアウォールポリシーの除外設定の条件に一致するトラフィックには適用されません。

5. ポリシーに使用するファイアウォール機能を選択します。

   - ファイアウォールが送信パケットをブロックすると、ファイアウォール違反通知メッセージが表示されます。メッセージを変更するには、563 ページの「ファイアウォール通知メッセージの内容の変更」を参照してください。
   - 管理者がすべてのファイアウォール機能を有効にし、ファイアウォールの設定権限をセキュリティエージェントユーザに付与した場合、ユーザはセキュリティエージェントコンソールで機能を有効または無効にしたり、ファイアウォール設定を変更したりできます。

     警告!

     管理者が Apex One の Web コンソールを使用して、ユーザが設定したセキュリティエージェントコンソール設定を無効にすることができなくなります。

   - この機能を有効にしない場合、Apex One の Web コンソールで指定するファイアウォール設定は、セキュリティエージェントコンソールの [ネットワークカードのリスト] の下に表示されます。
   - セキュリティエージェントコンソールの [ファイアウォール] タブの [設定] の下にある情報には、サーバの Web コンソールからの設定ではなく、セキュリティエージェントコンソールからの設定が常に反映されます。

6. ローカルまたはグローバルのソフトウェア安全性評価リストを有効にします。

   注意

   このサービスを有効にする前に、不正変更防止サービスとソフトウェア安全性評価サービスが有効であることを確認してください。

7. [除外] でファイアウォールポリシーの除外設定を選択します。ここに含まれるポリシーの除外設定は、ファイアウォール除外テンプレートに基づいています。詳細については、547 ページの「ファイアウォール除外テンプレートの編集」を参照してください。

   - ポリシーの除外名をクリックし、開いたページで設定を変更して、既存のポリシーの除外設定を変更してください。

注意

変更されたポリシーの除外設定は、これから作成されるポリシーにのみ適用されます。ポリシーの除外設定に対する変更を常に適用したい場合は、ファイアウォール除外テンプレートでポリシーの除外設定に対して同じ変更を行う必要があります。

- [追加] をクリックして、新しいポリシーの除外設定を作成します。開いたページで設定を指定します。

注意

ポリシーの除外設定は、これから作成されるポリシーにのみ適用されます。このポリシーの除外設定を他のポリシーに適用したい場合は、ファイアウォール除外テンプレートにあるポリシーの除外設定リストにまずこのポリシーを追加する必要があります。

8. [保存] をクリックします。

既存のファイアウォールポリシーの変更

手順

1. [エージェント] > [ファイアウォール] > [ポリシー] に移動します。
2. ポリシーをクリックします。
3. 次の項目を変更します。
   - ポリシー名
   - セキュリティレベル
   - ポリシーに使用するファイアウォール機能
   - ソフトウェアサービス安全性評価リストのステータス
   - ポリシーに含めるファイアウォールポリシーの除外設定
     - ポリシーの除外名をクリックし、開いたページで設定を変更して、既存のポリシーの除外設定を編集してください。

- [追加] をクリックして、新しいポリシーの除外設定を作成します。開いたページで設定を指定します。

4. [保存] をクリックして、既存のポリシーに変更を適用します。

ファイアウォール除外テンプレートの編集

ファイアウォール除外テンプレートには、セキュリティエージェントエンドポイントのポート番号または IP アドレスに基づいてさまざまな種類のネットワークトラフィックを許可またはブロックするよう設定できるポリシーの除外設定が含まれます。ポリシーの除外設定を作成してから、ポリシーの除外設定が適用されるポリシーを編集します。

使用するポリシーの除外設定の種類を決定します。2 種類の設定があります。

- 制限

  指定された種類のネットワークトラフィックのみをブロックし、すべてのネットワークトラフィックを許可するポリシーに適用します。制限ポリシー除外の一例は、トロイの木馬がしばしば使用するポートなど、攻撃を受けやすいセキュリティエージェントポートをブロックすることです。

- 許可

  指定された種類のネットワークトラフィックのみを許可し、すべてのネットワークトラフィックをブロックするポリシーに適用します。たとえば、Apex One サーバおよび Web サーバのみにアクセスするセキュリティエージェントを許可することができます。許可するには、信頼されたポート (Apex One サーバとの通信に使用される) および HTTP 通信でセキュリティエージェントが使用するポートからのトラフィックを許可します。

  セキュリティエージェント待機ポート: [エージェント] > [エージェント管理] > [ステータス] の順に選択します。ポート番号は「基本的な情報」の下にあります。

  サーバ待機ポート:[管理] > [設定] > [エージェント接続] の順に選択します。ポート番号は「エージェント接続設定」の下にあります。

Apex One には、一連の初期設定のファイアウォールポリシー除外が搭載されており、変更または削除することができます。

表 13-1. 初期ファイアウォールポリシー除外

除外設定名	処理	プロトコル	ポート番号	方向
DNS	許可	TCP/UDP	53	送受信
NetBIOS	許可	TCP/UDP	137, 138, 139, 445	送受信
HTTPS	許可	TCP	443	送受信
HTTP	許可	TCP	80	送受信
Telnet	許可	TCP	23	送受信
SMTP	許可	TCP	25	送受信
FTP	許可	TCP	21	送受信
POP3	許可	TCP	110	送受信
LDAP	許可	TCP/UDP	389	送受信

注意

初期設定の除外設定は、すべてのエージェントに適用されます。初期設定の除外設定を特定のエージェントのみに適用したい場合は、除外設定を編集し、そのエージェントの IP アドレスを指定してください。

以前の Apex One バージョンからバージョンアップした場合は、LDAP 除外設定は使用できません。この除外設定が除外リストにない場合、手動で追加してください。

ファイアウォールポリシー除外設定の追加

新しい除外を追加するときは、Apex One サーバとセキュリティエージェント間の通信に使用するポートをブロックしないでください。

Apex One サーバとセキュリティエージェントで使用されている待機ポートを次の方法で特定できます。

- サーバ待機ポート: [管理] > [設定] > [エージェント接続] に移動します。ポート番号は「エージェント接続設定」の下にあります。
- セキュリティエージェント待機ポート: [エージェント] > [エージェント管理] に移動します。ポート番号は「基本的な情報」の下にあります。

手順

1. [エージェント] > [ファイアウォール] > [ポリシー] に移動します。
2. [除外テンプレートの編集] をクリックします。
3. [追加] をクリックします。
4. このポリシーの除外設定の新しい名前を入力します。
5. アプリケーションの種類を選択します。すべてのアプリケーションを選択することも、アプリケーションパスまたはレジストリキーを指定することもできます。

   注意

   名前とフルパスが入力されていることを確認します。除外するアプリケーションの指定ではワイルドカードはサポートされません。

6. ネットワークトラフィック上で Apex One が実行する処理 (除外条件に一致するトラフィックをブロックまたは許可) およびトラフィックの方向 (セキュリティエージェントエンドポイント上の送受信ネットワークトラフィック) を選択します。
7. TCP、UDP、ICMP、または ICMPv6 から、ネットワークプロトコルの種類を選択します。
8. 処理を実行するセキュリティエージェントエンドポイントのポートを指定します。
9. 除外に含めるセキュリティエージェントエンドポイントの IP アドレスを選択します。

   たとえば、すべてのネットワークトラフィック (送受信) を拒否することを選択していて、ネットワーク上の 1 つのエンドポイントの IP アドレスを入力している場合、ポリシーにこの除外設定があるすべてのセキュリ

ティエージェントはその IP アドレスとの間でデータの送受信ができなくなります。

- すべての IP アドレス: すべての IP アドレスを含めます。
- 単一 IP アドレス: IPv4 アドレス、IPv6 アドレス、またはホスト名を入力します。
- 範囲 (IPv4 または IPv6): IPv4 アドレスまたは IPv6 アドレスの範囲を入力します。
- 範囲 (IPv6): IPv6 アドレスのプレフィックスと長さを入力します。
- サブネットマスク: IPv4 アドレスとサブネットマスクを入力します。

10. [保存] をクリックします。

    新しい除外を追加した [除外テンプレートの編集] 画面が表示されます。

11. 次のいずれかのボタンをクリックして、新しい除外をリストに適用します。
    - テンプレートの変更を保存: 現在の除外設定テンプレートリストの設定を保存しますが、設定を既存のポリシーに適用しません。
    - 保存してすべての既存ポリシーに適用: 現在の除外テンプレートリストの設定を保存して、設定を既存のすべてのポリシーにただちに適用します。

ファイアウォールポリシー除外設定の変更

手順

1. [エージェント] > [ファイアウォール] > [ポリシー] に移動します。
2. [除外テンプレートの編集] をクリックします。
3. ポリシー除外をクリックします。
4. 次の項目を変更します。
    - ポリシー除外名

- アプリケーションの種類、名前、またはパス
- ネットワークトラフィック上で Apex One が実行する処理およびトラフィックの方向
- ネットワークプロトコルの種類
- ポリシーの除外設定のポート番号
- セキュリティエージェントエンドポイント IP アドレス

5. [保存] をクリックします。

ポリシー除外リストの設定の保存

手順

1. [エージェント] > [ファイアウォール] > [ポリシー] に移動します。
2. [除外テンプレートの編集] をクリックします。
3. 次の保存オプションから選択します。
   - テンプレートの変更を保存:現在のポリシー除外および設定で除外テンプレートを保存します。このオプションは、既存のポリシーではなく、今後作成されるポリシーに対するテンプレートに適用されます。
   - 保存してすべての既存ポリシーに適用:現在のポリシー除外および設定で除外テンプレートを保存します。このオプションは、既存のポリシーおよび今後作成されるポリシーに対するテンプレートに適用されます。

ファイアウォールプロファイル

ファイアウォールプロファイルを使用することにより、ポリシーを適用する前に単一エージェントまたはエージェントグループに設定しなければならない属性を選択できます。特定ドメインのプロファイルを作成、設定、または削除できるユーザの役割を作成できます。

ビルトインの管理者アカウントを使用しているユーザや完全な管理者権限を持つユーザは、[エージェントのセキュリティレベル/除外リストを上書き] オプションを有効にして、セキュリティエージェントのプロファイル設定をサーバ設定で置き換えることもできます。

プロファイルには、次のものが含まれます。

- 関連ポリシー: それぞれのプロファイルは 1 つのポリシーを使用します。
- エージェント属性: 以下の属性を持つセキュリティエージェントは関連ポリシーを適用します。
  - IP アドレス: 特定の IP アドレス、一定の範囲の IP アドレスに該当する IP アドレス、または指定されたサブネットに属する IP アドレスを持つセキュリティエージェント
  - ドメイン: 特定の Apex One ドメインに属するセキュリティエージェント
  - エンドポイント: 特定のエンドポイント名を持つセキュリティエージェント
  - プラットフォーム: 特定のプラットフォームを実行しているセキュリティエージェント
  - ログオン名: 指定されたユーザがログオンしたセキュリティエージェントエンドポイント
  - NIC の説明: NIC の説明に一致するセキュリティエージェントエンドポイント
  - エージェントの位置: セキュリティエージェントがオンラインかオフラインかを示します。

注意

Apex One サーバまたは参照サーバのいずれかに接続できる場合、セキュリティエージェントはオンラインで、どのサーバにも接続できない場合はオフラインです。

Apex One には、「オールアクセスポリシー」を使用する「オールエージェントプロファイル」という初期設定のプロファイルが用意されています。この初期設定のプロファイルを変更または削除できます。また、新しいプロファ

イルを作成することもできます。各プロファイルおよび現在のプロファイルステータスに関連付けられたポリシーを含めて、初期設定およびユーザが作成したファイアウォールプロファイルは、Web コンソールのファイアウォールプロファイルリストにすべて表示されます。プロファイルリストを管理し、すべてのプロファイルをセキュリティエージェントに配信します。セキュリティエージェントは、エージェントエンドポイントのすべてのファイアウォールプロファイルを保存します。

ファイアウォールプロファイルリストの設定

手順

1. [エージェント] > [ファイアウォール] > [プロファイル] に移動します。
2. ビルトインの管理者アカウントを使用しているユーザや完全な管理者権限を持つユーザについては、必要に応じて、[エージェントのセキュリティレベル/除外リストを上書き] オプションを有効にして、セキュリティエージェントのプロファイル設定をサーバ設定で置き換えます。
3. 新しいプロファイルを追加するには、[追加] をクリックします。既存のプロファイルを編集するには、プロファイル名を選択します。

   プロファイルの設定画面が表示されます。詳細については、555 ページの「ファイアウォールプロファイルの追加および編集」を参照してください。
4. 既存のプロファイルを削除するには、ポリシーの横のチェックボックスを選択し、[削除] をクリックします。
5. リスト内でプロファイルの順序を変更するには、移動するプロファイルの横にあるチェックボックスを選択して、[▲] または [▼] をクリックします。

   Apex One は、プロファイルリストに表示される順序で、ファイアウォールプロファイルをセキュリティエージェントに適用します。たとえば、エージェントが最初のプロファイルに一致する場合、Apex One はそのプロファイルに設定された処理をエージェントに適用します。Apex One はエージェントに設定されたその他のプロファイルについては無視します。

ヒント

ポリシーが排他的であればあるだけ、リストの上位に表示する必要があります。たとえば、単一エージェントに対して作成したポリシーは最上位に表示され、その後にその範囲のエージェント、ネットワークドメイン、およびすべてのエージェントが続きます。

6. 参照サーバを管理するには、[参照サーバリストの編集] をクリックします。参照サーバは、ファイアウォールのプロファイルを適用するときに、Apex One サーバの代わりとして動作するエンドポイントです。ネットワーク上のエンドポイントであれば、参照サーバとして使用することができます (詳細については、610 ページの「参照サーバ」を参照してください)。参照サーバを有効にした場合、Apex One では次の状態を想定します。

   - 参照サーバに接続されたセキュリティエージェントは、Apex One サーバと通信できない場合も含め、オンラインである。
   - オンラインのセキュリティエージェントに適用されるファイアウォールプロファイルが、参照サーバに接続されているセキュリティエージェントにも適用される。

注意

ビルトインの管理者アカウントを使用しているユーザ、または完全な管理者権限を持つユーザのみが、参照サーバリストを表示して設定できます。

7. 現在の設定を保存し、セキュリティエージェントにプロファイルを割り当てるには、次の手順を実行します。

   a. [エージェントのセキュリティレベル/除外リストを上書き] をオンまたはオフにします。このオプションは、すべてのユーザ設定のファイアウォール設定を上書きします。

   b. [エージェントにプロファイルを適用] をクリックします。すべてのセキュリティエージェントに対してプロファイルリストのすべてのプロファイルが割り当てられます。

8. プロファイルをセキュリティエージェントに正常に割り当てたことを確認するには、次の手順を実行します。

a. [エージェント] > [エージェント管理] に移動します。エージェントツリー表示ドロップダウンボックスで、[ファイアウォール表示] を選択します。

b. 緑のチェックマークが、エージェントツリーの [ファイアウォール] 列の下に付いていることを確認します。

c. エージェントが正しいファイアウォールポリシーを適用していることを確認します。ポリシーは、エージェントツリーの [ファイアウォールポリシー] 列の下に表示されます。

ファイアウォールプロファイルの追加および編集

セキュリティエージェントエンドポイントは、さまざまなレベルの保護を必要とする場合があります。ファイアウォールプロファイルを使用すると、関連ポリシーを適用するエージェントエンドポイントを指定できます。通常、使用中の各ポリシーに必要なプロファイルは 1 つです。

ファイアウォールプロファイルの追加

手順

1. [エージェント] > [ファイアウォール] > [プロファイル]に移動します。
2. [追加] をクリックします。
3. [このプロファイルを有効にする] をクリックして、Apex One がセキュリティエージェントにプロファイルを配信できるようにします。
4. プロファイルを識別する名前とオプションの説明を入力します。
5. このプロファイルのポリシーを選択します。
6. Apex One がポリシーを適用するエージェントエンドポイントを指定します。次の条件に基づき、エンドポイントを選択します。
   - IP アドレス
   - ドメイン: ボタンをクリックして開き、エージェントツリーからドメインを選択します。

注意

完全なドメイン権限を持つユーザのみが、ドメインを選択できます。

- エンドポイント名: ボタンをクリックして開き、エージェントツリーからセキュリティエージェントエンドポイントを選択します。
- プラットフォーム
- ログオン名
- NIC の説明: 説明の全部または一部を入力します。ワイルドカードは使用できません。

ヒント

NIC の説明は、一般に製造者名で始まるため、NIC カードの製造者を入力することをお勧めします。たとえば、「Intel」と入力すると、Intel 製の NIC はすべてこの基準を満たします。「Intel(R) Pro/100」など特定の NIC モデルを入力した場合、「Intel(R) Pro/100」で始まる NIC の説明のみが基準を満たします。

- エージェントの位置: 次のどちらかを選択します。
  - 内部 - セキュリティエージェントは、設定済みの参照サーバに接続できます。

    注意

    位置を設定するには、[参照サーバリストの編集] をクリックします。

    詳細については、610 ページの「参照サーバ」を参照してください。
  - 外部 - セキュリティエージェントは、設定済みの参照サーバに接続できません。

7. ファイアウォールのセキュリティレベルを変更または設定可能な除外リストを編集して指定した種類のトラフィックを許可する権限を、ユーザに付与するかどうかを選択します。

詳細については、542 ページの「ファイアウォールポリシー」を参照してください。

8. [保存] をクリックします。

ファイアウォールプロファイルの変更

手順

1. [エージェント] > [ファイアウォール] > [プロファイル] に移動します。
2. プロファイルをクリックします。
3. [このプロファイルを有効にする] をクリックして、セキュリティエージェントにこのプロファイルを配信できるようにします。次の項目を変更します。
   - プロファイル名および説明
   - プロファイルに割り当てられたポリシー
   - 次の条件に基づくセキュリティエージェントエンドポイント:
     - IP アドレス
     - ドメイン:ボタンをクリックしてエージェントツリーを開き、そこからドメインを選択します。
     - エンドポイント: ボタンをクリックしてエージェントツリーを開き、そこからエージェントエンドポイントを選択します。
     - プラットフォーム
     - ログオン名
     - NIC の説明:説明の全部または一部を入力します。ワイルドカードは使用できません。

> **ヒント**
>
> NIC の説明は、一般に製造者名で始まるため、NIC カードの製造者を入力することをお勧めします。たとえば、「Intel」と入力すると、Intel 製の NIC はすべてこの基準を満たします。「Intel(R) Pro/100」など特定の NIC モデルを入力した場合、「Intel(R) Pro/100」で始まる NIC の説明のみが基準を満たします。

- エージェントの状態

4. [保存] をクリックします。

ファイアウォール権限

ユーザに独自のファイアウォール設定を行う権限を付与します。ユーザが行う設定はすべて、Apex One サーバから配信される設定で上書きすることはできません。たとえば、ユーザがファイアウォールを無効にした場合、管理者が Apex One サーバでファイアウォールを有効にしても、セキュリティエージェントエンドポイントではファイアウォール機能は無効のままです。

ユーザにファイアウォールの設定を許可するには、次の設定を有効にします。

表 13-2. ファイアウォール権限

権限	説明
セキュリティエージェントコンソールにファイアウォール設定を表示	[ファイアウォール] オプションにはセキュリティエージェント上のすべてのファイアウォール設定が表示されます。

権限	説明
ユーザにファイアウォールおよび警告メッセージの有効化/無効化の変更を許可	Apex One のファイアウォールは、ステートフルインスペクション、高性能なネットワークウイルス検索、および駆除機能を使用して、ネットワーク上のエージェントとサーバを保護します。ファイアウォールとその機能を有効化または無効化する権限をユーザに付与する場合、エンドポイントが侵入やハッカーの攻撃にさらされることを防ぐため、長期間ファイアウォールを無効にしないよう、ユーザに注意してください。 この権限をユーザに付与しない場合、Apex One サーバの Web コンソールで行われたファイアウォール設定が、セキュリティエージェントコンソールの [ネットワークカード] の下に表示されます。
エージェントに Apex One サーバへのファイアウォールログの送信を許可	Apex One ファイアウォールでブロックおよび許可したトラフィックを分析するには、このオプションを選択します。 ファイアウォールログの詳細については、564 ページの「ファイアウォールログ」を参照してください。 このオプションを選択する場合、[セキュリティ設定] タブの [エージェント] > [グローバルエージェント設定] でログの送信スケジュールを設定します。[ファイアウォール設定] セクションに移動します。このスケジュールは、ファイアウォールログ送信権限を持つエージェントにのみ適用されます。手順については、560 ページの「グローバルファイアウォール設定」を参照してください。

ファイアウォール権限の付与

手順

1. [エージェント] > [エージェント管理]に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [権限] タブの [ファイアウォール] セクションに移動します。

5. ファイアウォール権限オプションを選択します。
6. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。
   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
   - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

グローバルファイアウォール設定

セキュリティエージェントにグローバルファイアウォール設定を適用する方法はいくつかあります。

- 特定のファイアウォール設定を、サーバが管理するすべてのエージェントに適用することができます。
- 設定を、特定のファイアウォール権限を持つセキュリティエージェントにのみ適用することができます。たとえば、ファイアウォールログの送信スケジュールは、ログをサーバに送信する権限を持つセキュリティエージェントのみに適用されます。

グローバルファイアウォール設定

手順

1. [エージェント] > [グローバルエージェント設定]に移動します。
2. [セキュリティ設定] タブの [ファイアウォール設定] に移動し、次の項目を設定します。

設定	説明
Apex One ファイアウォールを有効にする	ポリシーやプロファイルを適用するには、Apex One ファイアウォールをすべてのセキュリティエージェントで有効にする必要があります。
ファイアウォールログをサーバに送信する間隔	ファイアウォールログを Apex One サーバに送信する権限を、特定のセキュリティエージェントに付与することができます。このセクションでログ送信スケジュールを設定します。ファイアウォールログを送信する権限を持つエージェントだけがこのスケジュールを使用します。 選択したエージェントで使用可能なファイアウォール権限については、558 ページの「ファイアウォール権限」を参照してください。
システムの再起動後に Apex One ファイアウォールドライバをアップデートする	セキュリティエージェントで、セキュリティエージェントエンドポイントの再起動後にのみファイアウォールドライバをアップデートできるようにします。エージェントバージョンアップ時のファイアウォールドライバのアップデートにおいて、ネットワークからの一時的な切断といったエージェントエンドポイントの潜在的な問題を回避するには、このオプションを有効にします。
ファイアウォールログの件数情報を Apex One サーバに 1 時間ごとに送信して、大規模感染が発生する可能性があるかどうかを確認する	このオプションを有効にすると、セキュリティエージェントは、1 時間ごとに Apex One サーバにファイアウォールログ件数を送信します。 ファイアウォールログの詳細については、564 ページの「ファイアウォールログ」を参照してください。 Apex One は、ログ件数とファイアウォール違反大規模感染の条件を使用して大規模感染の可能性を判断します。Apex One は、大規模感染の発生時には Apex One 管理者にメール通知を送信します。

3. [システム] タブの [ソフトウェア安全性評価サービスの設定] に移動し、[挙動監視、ファイアウォール、ウイルス対策検索に対してソフトウェア安全性評価サービスを有効にする] を選択します。

   ソフトウェア安全性評価サービスでは、不正プログラム挙動ブロック、イベント監視、ファイアウォール、またはウイルス対策検索で検出されたプログラムに関するクエリがトレンドマイクロのデータセンターに送信され、プログラムの安全性が確認されます。ソフトウェア安全性評価

サービスを有効にすることによって、誤検出の確率を低くすることができます。

注意

ソフトウェア安全性評価サービスを有効にする前に、セキュリティエージェントのプロキシ設定 (詳細については、687 ページの「セキュリティエージェントプロキシ設定」を参照) が正しく行われていることを確認してください。プロキシ設定の誤りやインターネット接続の中断は、トレンドマイクロのデータセンターから送信される応答の延期や不達の原因となり、監視対象のプログラムが応答していないように見えます。

また、IPv6 セキュリティエージェントでは、トレンドマイクロのデータセンターに直接クエリを送信することはできません。このようなセキュリティエージェントがトレンドマイクロのデータセンターに接続できるようにするには、IP アドレスを変換可能な DeleGate などのデュアルスタックプロキシサーバが必要です。

4. [保存] をクリックします。

セキュリティエージェントユーザ向けのファイアウォール違反通知

Apex One では、ファイアウォールポリシーに違反する送信トラフィックをブロックした直後にエンドポイントに通知メッセージを表示できます。通知メッセージを有効/無効にする権限をユーザに付与します。

注意

この通知メッセージは、特定のファイアウォールポリシーの設定時にも有効にできます。ファイアウォールポリシーを設定するには、544 ページの「ファイアウォールポリシーの追加」を参照してください。

通知メッセージを有効化/無効化する権限のユーザへの付与

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [権限] タブの [ファイアウォール] セクションに移動します。
5. [ユーザにファイアウォールおよび警告メッセージの有効化/無効化の変更を許可] を選択します。
6. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。
   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
   - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

ファイアウォール通知メッセージの内容の変更

手順

1. [管理] > [通知] > [エージェント] に移動します。
2. [種類] のドロップダウンから、[ファイアウォール違反] を選択します。

3. 表示されたテキストボックスで初期設定のメッセージを変更します。
4. [保存]をクリックします。

ファイアウォールログ

サーバで使用可能なファイアウォールログは、ファイアウォールログの送信権限を持つセキュリティエージェントによって送信されます。特定のエージェントにこの権限を付与して、Apex One ファイアウォールがブロックしているエンドポイント上のトラフィックを監視および分析します。

ファイアウォール権限の詳細については、558 ページの「ファイアウォール権限」を参照してください。

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログの削除スケジュールを設定します。ログの管理方法の詳細については、616 ページの「ログ管理」を参照してください。

ファイアウォールログの表示

セキュリティエージェントは、ファイアウォール違反の検出時にログを生成し、サーバにログを送信します。

手順

1. 次のいずれかに移動します。
   - [ログ] > [エージェント] > [セキュリティリスク]
   - [エージェント] > [エージェント管理]
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [ファイアウォールログ条件] 画面に移動します。

- [セキュリティリスクログ] 画面で、[ログの表示] > [ファイアウォールログ] の順にクリックします。
- [エージェント管理] 画面で、[ログ] > [ファイアウォールログ] の順にクリックします。

4. 最新のログが使用可能であるかを確認するには、[エージェントに通知する] をクリックします。エージェントがファイアウォールログを送信して次の手順に進むまでには、しばらく時間がかかります。
5. ログの条件を指定して [ログを表示する] をクリックします。
6. ログが表示されます。ログには、次の情報が含まれています。

項目	説明
日時	検出された日時
エンドポイント	検出が行われたエンドポイント
ドメイン	検出が発生したドメイン
リモートホスト	リモートホストの IP アドレス
ローカルホスト	ローカルホストの IP アドレス
プロトコル	使用するプロトコル
ポート番号	ポート番号
方向	• 受信: 受信トラフィックを示します。 • 送信: 送信トラフィックを示します。
プロセス名	ファイアウォール違反が発生したエンドポイントで実行可能なプログラムまたは実行されているサービス
説明	実際のセキュリティリスク (ネットワークウイルス、IDS 攻撃など) またはファイアウォールポリシー違反を指定します。

7. ログを CSV ファイルに保存するには、[CSV 形式ですべてエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。

ファイアウォール違反アウトブレーク

ファイアウォール違反アウトブレークをファイアウォール違反の検出数と検出期間によって定義します。

Apex One には、Apex One 管理者に大規模感染について通知する初期設定のメッセージが用意されています。通知メッセージは要求に合わせて変更できます。

注意

Apex One では、ファイアウォールアウトブレーク通知をメールで送信できます。Apex One から正常にメールが送信されるように、メールを設定します。詳細については、612 ページの「管理者通知設定」を参照してください。

ファイアウォール違反アウトブレークの基準と通知の設定

手順

1. [管理] > [通知] > [アウトブレーク]に移動します。
2. [条件] タブで次の操作を実行します。
   a. [ファイアウォール違反] セクションに移動します。
   b. [セキュリティエージェントでファイアウォール違反を監視] を選択します。
   c. 不正侵入検知ログ、ファイアウォールログ、ネットワークウイルスログの件数を指定します。
   d. 検出期間を指定します。

ヒント

この画面では初期設定値を使用することをお勧めします。

Apex One は、このログ数を超えたとき通知メッセージを送信します。たとえば、不正侵入検知ログ、ファイアウォールログ、ネットワークウイ

ルスログをそれぞれ 100 件に指定し、期間を 3 時間に指定した場合、サーバが 301 件のログを 3 時間以内に受信すると、Apex One から通知が送信されます。

3. [メール] タブで次の操作を実行します。

   a. [ファイアウォール違反アウトブレーク] セクションに移動します。

   b. [メールによる通知を有効にする] を選択します。

   c. メールの受信者を指定します。

   d. 初期設定のメールの件名およびメッセージをそのまま使用するか変更します。[件名] および [メッセージ] では、トークン変数を使用してデータを表現できます。

   表 13-3. ファイアウォール違反アウトブレーク通知のトークン変数

変数	説明
%A	規定数を超えたログの種類
%C	ファイアウォール違反ログの数
%T	ファイアウォール違反ログを累積する期間

4. [保存]をクリックします。

Apex One ファイアウォールのテスト

Apex One ファイアウォールが正常に機能することを確認するために、単一のセキュリティエージェントまたはセキュリティエージェントグループでテストを行います。

警告!

セキュリティエージェントプログラムの設定は、制御された環境でのみテストしてください。ネットワークまたはインターネットに接続しているエンドポイント上ではテストしないでください。これにより、セキュリティエージェントエンドポイントが、ウイルス、ハッカーの攻撃、またはその他のリスクにさらされる可能性があります。

手順

1. テストポリシーを作成して保存します。テストするトラフィックの種類をブロックするよう設定します。たとえば、セキュリティエージェントがインターネットにアクセスしないようにするには、次の処理を実行します。

   a. セキュリティレベルを [低] に設定します (すべての受信/送信トラフィックを許可)。

   b. [ファイアウォールを有効にする] および [ファイアウォール違反の検出時に通知を表示する] を選択します。

   c. HTTP (または HTTPS) トラフィックをブロックする除外設定を作成します。

2. テストプロファイルを作成して保存し、ファイアウォール機能をテストするエージェントを選択します。テストポリシーをテストプロファイルに関連付けます。

3. [エージェントにプロファイルを適用] をクリックします。

4. 配信を確認します。

   a. [エージェント] > [エージェント管理] の順にクリックします。

   b. エージェントが属するドメインを選択します。

   c. エージェントツリー表示から、[ファイアウォール表示] を選択します。

   d. エージェントツリーの [ファイアウォール] 列の下に緑色のチェックマークが付いているかを確認します。

   e. エージェントが正しいファイアウォールポリシーを適用していることを確認します。ポリシーは、エージェントツリーの [ファイアウォールポリシー] 列の下に表示されます。

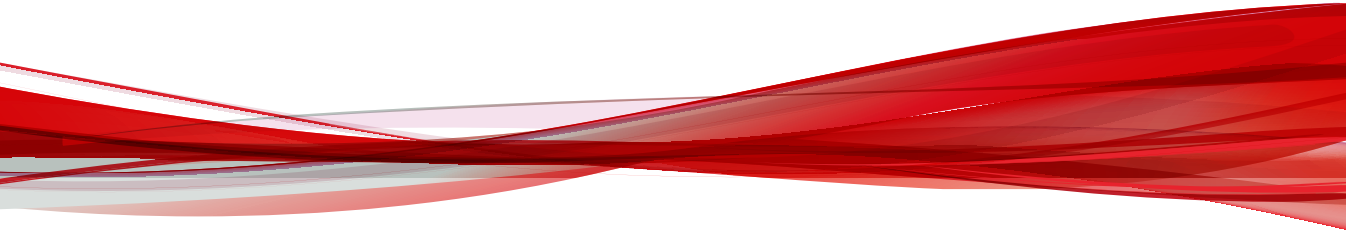
5. ポリシーで設定した種類のトラフィックの送信または受信を試行して、エージェントエンドポイントのファイアウォールをテストします。

6. エージェントがインターネットにアクセスしないように設定したポリシーをテストするには、エージェントエンドポイントで Web ブラウザを

開きます。ファイアウォール違反の通知メッセージを表示するよう設定した場合は、送信トラフィックの侵害が発生すると、エージェントエンドポイントにメッセージが表示されます。

パート III

Apex One サーバおよびエージェントの管理



第 14 章

Apex One サーバの管理

この章では、Apex One サーバの管理と設定について説明します。

この章は次のトピックで構成されます。

役割ベースの管理

役割ベースの管理は、Web コンソールへのアクセス権の付与および制御を行うために使用します。組織内に複数の Apex One 管理者がいる場合は、この機能を使用することで、管理者に特定の Web コンソール権限を割り当てて、特定のタスクの実行に必要なツールと権限のみを提供できます。1 つまたは複数の管理対象のドメインを割り当てることによって、エージェントツリーへのアクセスを制御することもできます。さらに、管理者以外には Web コンソールに対する表示専用のアクセス権を付与することもできます。

それぞれのユーザ（管理者または非管理者）に特定の役割を割り当てます。役割によって、Web コンソールへのアクセスレベルが定義されます。ユーザは、カスタムユーザアカウント、または Active Directory アカウントを使用して Web コンソールにログオンします。

役割ベースの管理には、次のタスクがあります。

1. ユーザの役割の定義。詳細については、586 ページのユーザの役割を参照してください。
2. ユーザアカウントの設定および各ユーザアカウントへの特定の役割の割り当て。詳細については、575 ページのユーザアカウントを参照してください。

すべてのユーザが Web コンソールで行った処理は、システムイベントログで確認できます。次の処理がログに記録されます。

- コンソールへのログオン
- パスワードの変更
- コンソールからのログオフ
- セッションタイムアウト (ユーザは自動的にログオフされます)

ユーザアカウント

ユーザアカウントを手動で設定するか、Active Directory アカウントを使用して、エージェントツリー内で使用できる詳細なエージェント設定、タスク、およびデータを表示または設定するための権限を割り当てます。各ユーザに

特定の役割を割り当てる必要があります。これにより、ユーザが表示または設定できる Web コンソールのメニュー項目が決まります。Apex One のユーザアカウントを使用して、Trend Micro Apex Central コンソールから Apex One への「シングルサインオン」を実行できます。

Apex One サーバのインストール時に、「root」というビルトインのアカウントが自動的に作成されます。ルートアカウントを使用してログオンするユーザは、すべてのメニュー項目にアクセスできます。ルートアカウントは削除できませんが、パスワードやアカウントの説明などのアカウントの詳細は変更できます。ルートアカウントのパスワードを忘れた場合は、パスワードの再設定についてサポート担当者にお問い合わせください。

注意

Apex One サーバをバージョンアップした場合、以前に追加したカスタムアカウントについては、[ステップ 3 エージェントツリーメニューの定義] 画面でカスタムアカウントを編集し、すべての新機能を手動で有効にする必要があります。

権限の詳細については、583 ページの「ドメインの権限の定義」を参照してください。

次の表は、[ユーザアカウント] 画面で使用できるタスクを示しています。

タスク	説明
アカウントの追加	[追加] をクリックして、新しいユーザアカウントを作成します。 詳細については、579 ページの「ユーザアカウントの追加」を参照してください。
既存のアカウントの削除	既存のユーザアカウントを選択して、[削除] をクリックします。
既存のアカウントの編集	既存のユーザアカウントの名前をクリックして、現在のアカウント設定を表示または変更します。

エージェント管理メニュー項目

次の表は、使用可能なエージェント管理メニュー項目のリストです。

注意

メニュー項目は、そのプラグインプログラムをアクティベートしないと表示されません。たとえば、情報漏えい対策モジュールがアクティベートされていない場合、情報漏えい対策のメニュー項目はリストに表示されません。

表 14-1. エージェント管理メニュー項目

メインメニュー項目	サブメニュー
ステータス	なし
タスク	• ScanNow • エージェントのアンインストール • 隔離の一括復元 • スパイウェア/グレーウェアの復元

メインメニュー項目	サブメニュー

設定	• 検索設定
	  • 検索方法
	  • 手動検索設定
	  • リアルタイム検索設定
	  • 予約検索設定
	  • ScanNow 設定
	• Web レピュテーション設定
	• 不審接続監視設定
	• 挙動監視設定
	• デバイスコントロール設定
	• 情報漏えい対策設定
	• サンプル送信
	• アップデートエージェント設定
	• 権限とその他の設定
	• 追加サービス設定
	• スパイウェア/グレーウェアの承認済みリスト
	• 信頼済みプログラムリスト
	• 機械学習型検索設定
	• 設定のエクスポート
	• 設定のインポート

メインメニュー項目	サブメニュー
ログ	• ウイルス/不正プログラムログ • スパイウェア/グレーウェアログ • ファイアウォールログ • Web レピュテーションログ • 不審接続監視ログ • 不審ファイルログ • C&C コールバックログ • 挙動監視ログ • 機械学習型検索ログ • デバイスコントロールログ • 情報漏えい対策ログ • 検索ログ • ログの削除
エージェントツリーの管理	• ドメインの追加 • ドメイン名の変更 • エージェントの移動 • ドメイン/エージェントの削除
エクスポート	なし

ユーザアカウントの追加

ユーザアカウントを手動で設定するか、Active Directory アカウントを使用して、エージェントツリー内で使用できる詳細なエージェント設定、タスク、およびデータを表示または設定するための権限を割り当てます。

手順

1. [管理] > [アカウント管理] > [ユーザアカウント] に移動します。
2. [追加] をクリックします。

   [ステップ 1 ユーザ情報] 画面が表示されます。
3. [このアカウントを有効にする] を選択します。
4. [役割の選択] ドロップダウンで、前に設定した役割を選択します。

   詳細については、588 ページの「カスタムの役割の追加」を参照してください。
5. [ユーザ情報] で、次の項目を設定します。
   - カスタムアカウント: ユーザアカウントを手動で作成する場合に選択し、必要な情報を指定します。
     - ユーザ名: アカウントの一意のユーザ名を入力します。
     - 説明: アカウントの説明を入力します。
     - パスワード: アカウントが Apex One Web コンソールへのログオンに使用するパスワードと確認用のパスワードを入力します。

       重要

       パスワードは以下の複雑さの要件を満たしている必要があります。
       - 8～32 文字の長さ
       - 大文字 (A～Z)、小文字 (a～z)、数字 (0～9)、特殊文字をそれぞれ 1 文字以上含む
       - ユーザ名を含まない
       - 印刷できない ASCII 文字を含まない
   - メールアドレス: ユーザアカウントに関連付けられているメールアドレスを入力します。

注意

Apex One の通知はこのメールアドレスに送信されます。通知によって、受信者にセキュリティリスクの検出や、デジタル資産の転送について知らせます。

通知の詳細については、351 ページの「管理者向けのセキュリティリスクの通知」を参照してください。

- Active Directory ユーザまたはグループ: 既存の Active Directory アカウントまたはグループを使用して Apex One Web コンソールにログオンする場合に選択します。

重要

ユーザアカウントを管理するためには、Apex One サーバが Active Directory ドメインに属している必要があります。

a. [ユーザ名またはグループ] に、使用する Active Directory アカウントを入力します。

b. [ドメイン] に、[ユーザ名またはグループ] が属する Active Directory ドメインを入力します。

c. [検索] をクリックします。

d. [ユーザおよびグループ] リストで、検索結果からアカウントを選択し、[>] をクリックして [選択されたユーザおよびグループ] リストに追加します。

6. [次へ] をクリックします。

   [ステップ 2 エージェントドメイン制御] 画面が表示されます。

7. すべての Apex One ドメインの表示を許可するルートアカウントを選択するか、またはユーザアカウントがエージェントツリー内でアクセス可能な特定の Apex One ドメインを選択します。

重要

ユーザアカウントがエージェントツリーにアクセスしたときに Apex One に表示されるのは、選択されたドメインのみです。ドメインを選択しない場合、Apex One ではエージェントツリー上のドメインが非表示になります。

8. [次へ] をクリックします。

   [ステップ 3 エージェントツリーメニューの定義] 画面が表示されます。

9. [使用可能なメニュー項目] をクリックして、使用可能なメニュー項目のそれぞれに権限を指定します。使用可能なメニュー項目の一覧は、576 ページの「エージェント管理メニュー項目」を参照してください。

   手順 8 で設定したエージェントツリー範囲によって、メニュー項目に対する権限レベルが決まり、権限の対象が定義されます。エージェントツリー範囲は、ルートドメイン (すべてのエージェント)、または指定したエージェントツリードメインのどちらかです。

表 14-2. エージェント管理メニュー項目とエージェントツリー範囲

条件	エージェントツリー範囲	
	ルートドメイン	特定のドメイン
メニュー項目の権限	設定、表示、またはアクセス拒否	設定、表示、またはアクセス拒否

条件	エージェントツリー範囲	
	ルートドメイン	特定のドメイン
対象	ルートドメイン (すべてのエージェント) または特定のドメイン たとえば、エージェントツリーの [タスク] メニュー項目に対する [設定] 権限を役割に付与できます。対象がルートドメインの場合、ユーザはすべてのエージェントに対してタスクを開始できます。対象がドメイン A および B の場合は、ドメイン A と B に属するエージェントに対してのみタスクを開始できます。	選択したドメインのみ たとえば、エージェントツリーの [設定] メニュー項目に対する [設定] 権限を役割に付与できます。この場合、ユーザは選択したドメイン内のエージェントにのみ設定を配信できます。
	エージェントツリーは、[サーバ/エージェントのメニュー項目] の [エージェント管理] メニュー項目に対する権限が [表示] の場合にのみ表示されます。	

- [設定] の下のチェックボックスをオンにすると、[表示] の下のチェックボックスも自動的にオンになります。
- どのチェックボックスもオンにしなかった場合、権限は [アクセス拒否] になります。
- ドメインを選択して権限を設定している場合、[選択したドメインの設定を他のドメインにコピー] をクリックして他のドメインに権限をコピーできます。

10. [完了] をクリックします。
11. ユーザにアカウントの詳細を送信します。

ドメインの権限の定義

ドメインの権限を定義する場合、親ドメインの権限が、その管理対象であるすべてのサブドメインに自動的に適用されます。サブドメインに親ドメインよりも低い権限を付与することはできません。たとえば、システム管理者に

Apex One で管理するすべてのセキュリティエージェント (「Apex One サーバ」ドメイン) を表示および設定する権限がある場合、各サブドメインの権限でもシステム管理者にこれらの設定機能へのアクセス許可する必要があります。あるサブドメインからいずれかの権限を削除すると、システム管理者はすべてのセキュリティエージェントに対する設定権限は持たないことになります。

以下の手順では、次のドメインツリーを使用します。

たとえば、ユーザアカウント「Chris」に対して、サブドメイン「Employees」の特定のメニュー項目を表示および設定する権限と、親ドメイン「Managers」のログを表示するだけの権限を付与するには、次の手順を実行します。

表 14-3. ユーザアカウント「Chris」の権限

ドメイン	必要な権限
Apex One サーバ	特に必要なし
Managers	[ログ] の表示
Employees	[タスク] の表示および設定 [ログ] の表示および設定 [設定] の表示
Sales	特に必要なし

手順

1. [ユーザアカウント: ステップ 3 エージェントツリーメニューの定義] 画面に移動します。
2. 「Apex One サーバ」ルートドメインをクリックします。

3. [表示] チェックボックスと [設定] チェックボックスをすべてオフにします。

   注意

   「Apex One サーバ」ドメインを設定できるのは、すべてのサブドメインを [ユーザアカウント: ステップ 2 エージェントドメイン制御] 画面で選択した場合のみです。

4. 「Sales」ドメインをクリックします。
5. [表示] チェックボックスと [設定] チェックボックスをすべてオフにします。

   注意

   「Sales」ドメインが表示されるのは、[ユーザアカウント: ステップ 2 エージェントドメイン制御] 画面で選択した場合のみです。

6. 「Managers」ドメインをクリックします。
7. 「ログの表示」を選択し、その他の [表示] チェックボックスと [設定] チェックボックスをすべてオフにします。
8. 「Employees」ドメインをクリックします。
9. Chris に対して、次のメニュー項目を選択します。
   - タスク:表示および設定
   - ログ:表示および設定
   - 設定:表示

   これで、Chris は、「Employees」ドメインでは選択されたメニュー項目を表示および設定でき、「Managers」ドメインでは [ログ] の表示のみが可能です。

Chris に「Managers」ドメインを表示および設定する権限を付与すると、「Employees」サブドメインに対しても同じ権限が自動的に付与されます。これは、「Managers」ドメインがそのすべてのサブドメインを管理するためです。

ユーザの役割

特定のユーザアカウントによる特定の Web コンソール画面へのアクセスを制限するには、ユーザの役割を定義して割り当てます。Web コンソール画面を完全に非表示にする、アクセス権限を「読み取り専用」に制限する、またはすべての設定権限を付与するようにユーザの役割を定義できます。

次の表は、[ユーザの役割] 画面で使用できるタスクを示しています。

タスク	説明
カスタムの役割の追加	[追加] をクリックして、新しいカスタムの役割を作成します。 詳細については、588 ページの「カスタムの役割の追加」を参照してください。 **重要** 「ルート」アカウントまたは管理者 (ビルトイン) の役割を持つユーザのみが、カスタムのユーザの役割を作成してユーザアカウントに割り当てることができます。
既存のカスタムの役割からの設定のコピー	既存のカスタムの役割を選択して、[コピー] をクリックします。[役割のコピー] 画面が表示され、初期設定に基づいて新しいカスタムの役割を作成できます。
既存のカスタムの役割の削除	既存のカスタムの役割を選択して、[削除] をクリックします。 **重要** ユーザアカウントに現在割り当てられている役割を削除することはできません。

タスク	説明
カスタムの役割のエクスポート	既存のカスタムの役割を選択して [エクスポート] ボタンをクリックし、次のいずれかを選択します。 • DAT 形式でエクスポート: 選択した役割を DAT ファイルにエクスポートします。このファイルは別の Apex One サーバにインポートできます。 • CSV 形式でエクスポート: 選択した役割を CSV ファイルにエクスポートします。このファイルを使用して役割設定を確認できます。 **重要** 生成した CSV ファイルを Apex One サーバにインポートすることはできません。
カスタムの役割のインポート	[インポート] をクリックして、以前にエクスポートしたユーザの役割の DAT ファイルからユーザの役割設定をインポートします。 詳細については、594 ページの「カスタムの役割のインポートまたはエクスポート」を参照してください。
既存のカスタムの役割の編集	既存のユーザの役割の名前をクリックして、現在の役割設定を表示または変更します。 **注意** 事前定義済みのユーザの役割の内容を変更することはできません。 詳細については、587 ページの「ビルトインのユーザの役割」を参照してください。

ビルトインのユーザの役割

Apex One には一連のビルトインのユーザの役割が用意されており、これは変更または削除することができません。ビルトインの役割は次のとおりです。

表 14-4. ビルトインのユーザの役割

役割名	説明
管理者	この役割は、他の Apex One 管理者または Apex One について十分な知識を持つユーザに委任します。 この役割を持つユーザは、すべてのメニュー項目に対する「設定」の権限が付与されます。 **注意** 「管理者 (ビルトイン)」の役割が割り当てられたユーザのみがプラグインメニュー項目にアクセスできます。

ゲストユーザ	この役割は、Web コンソールを参照用に表示するユーザに委任します。
	• ゲストユーザの役割を持つユーザは、次のメニュー項目にはアクセスできません。
	  • プラグイン
	  • [管理] > [アカウント管理] > [ユーザの役割]
	  • [管理] > [アカウント管理] > [ユーザアカウント]
	• ユーザには、他のすべてのメニュー項目に対する「表示」の権限が付与されます。

カスタムの役割の追加

使用可能なビルトインの役割に要件を満たすものがない場合は、新しいカスタムユーザの役割を追加します。

詳細については、587 ページの「ビルトインのユーザの役割」を参照してください。

手順

1. [管理] > [アカウント管理] > [ユーザの役割] に移動します。
2. [追加] をクリックします。

   [役割の追加] 画面が表示されます。

3. [役割情報] で、次の項目を指定します。
   - 名前: 役割の一意の名前を入力します。
   - 説明: (オプション)
4. [役割のアクセス権限] で、次の手順を実行します。
   a. 役割が割り当てられているユーザアカウントがアクセス可能なメニュー項目を選択します。
      - サーバ/エージェントのメニュー項目: セキュリティエージェントと Apex One サーバのグローバルな設定、タスク、およびデータが含まれています。

        詳細については、590 ページの「サーバおよびエージェントのメニュー項目」を参照してください。
      - 管理下のドメインのメニュー項目: エージェントツリー以外で使用可能な、詳細なセキュリティエージェント設定、タスク、およびデータが含まれています。

        詳細については、593 ページの「管理下のドメインのメニュー項目」を参照してください。

   b. 役割が割り当てられているユーザアカウントの選択されたメニュー項目に対するアクセス権限を選択します。
      - 設定: メニュー項目へのフルアクセスを許可します。

        ユーザはメニュー項目ですべての設定の指定、すべてのタスクの実行およびデータの表示を行うことができます。
      - 表示: ユーザはメニュー項目の設定、タスクおよびデータの表示のみが許可されます。

注意

メニュー項目を完全に非表示にするには、[設定] チェックボックスと [表示] チェックボックスをオフにします。これで、役割が割り当てられているユーザアカウントにはメニュー項目が表示されなくなります。

5. [保存] をクリックします。

   新しい役割が [ユーザの役割] 画面に表示されます。

サーバおよびエージェントのメニュー項目

次の表は、サーバ/エージェントの使用可能なメニュー項目のリストです。

注意

メニュー項目は、そのプラグインプログラムをアクティベートしないと表示されません。たとえば、情報漏えい対策モジュールがアクティベートされていない場合、情報漏えい対策のメニュー項目はリストに表示されません。追加のプラグインプログラムはプラグインメニュー項目の下に表示されます。

「管理者 (ビルトイン)」の役割が割り当てられたユーザのみがプラグインメニュー項目にアクセスできます。

表 14-5. エージェントメニュー項目

トップレベルのメニュー項目	メニュー項目
エージェント	• エージェント管理 • エージェントのグループ設定 • グローバルエージェント設定 • エンドポイントの位置 • 情報漏えい対策 • 接続状態の確認 • 大規模感染予防サービス

表 14-6. ログメニュー項目

トップレベルのメニュー項目	メニュー項目

ログ	• エージェント
	  • セキュリティリスク
	  • コンポーネントアップデート
	• サーバアップデート
	• システムイベント
	• ログ管理

表 14-7. アップデートメニュー項目

トップレベルのメニュー項目	メニュー項目	サブメニュー項目
アップデート	サーバ	• 予約アップデート • 手動アップデート • アップデート元
	エージェント	• 自動アップデート • アップデート元
	ロールバック	なし

表 14-8. 管理メニュー項目

トップレベルのメニュー項目	メニュー項目	サブメニュー項目
管理	アカウント管理	• ユーザアカウント • ユーザの役割

トップレベルのメニュー項目	メニュー項目	サブメニュー項目
		注意 [ユーザアカウント] と [ユーザの役割] には、ビルトインの管理者アカウントを使用するユーザのみがアクセスできます。
	Smart Protection	• Smart Protection ソース • 統合サーバ • スマートフィードバック
	Active Directory	• Active Directory 統合 • 予約同期
	通知	• 一般設定 • アウトブレーク • エージェント
	設定	• プロキシ • エージェント接続 • オフラインエージェント • 隔離フォルダ設定 • 製品ライセンス • Apex Central • Web コンソール • データベースバックアップ • 不審オブジェクトリスト • エッジリレー • サーバの移行

管理下のドメインのメニュー項目

次の表は、管理下のドメインの使用可能なメニュー項目のリストです。

表 14-9. ダッシュボードメニュー項目

メインメニュー項目	メニュー項目
ダッシュボード 注意 このページには、権限に関係なくすべてのユーザがアクセスできます。	なし

表 14-10. 診断メニュー項目

トップレベルのメニュー項目	メニュー項目	サブメニュー項目
診断	セキュリティコンプライアンス	• 手動レポート • 予約レポート
	管理対象外のエンドポイント	なし

表 14-11. エージェントメニュー項目

トップレベルのメニュー項目	メニュー項目	サブメニュー項目
エージェント	ファイアウォール	• ポリシー • プロファイル
	エージェントのインストール	• ブラウザベース • リモート

表 14-12. ログメニュー項目

トップレベルのメニュー項目	メニュー項目	サブメニュー項目
ログ	エージェント	• 接続状態の確認 • 隔離の一括復元 • スパイウェア/グレーウェアの復元

表 14-13. アップデートメニュー項目

トップレベルのメニュー項目	メニュー項目	サブメニュー項目
アップデート	概要	なし
	エージェント	手動アップデート

表 14-14. 管理メニュー項目

トップレベルのメニュー項目	メニュー項目	サブメニュー項目
管理	通知	管理者

カスタムの役割のインポートまたはエクスポート

手順

1. [管理] > [アカウント管理] > [ユーザの役割] に移動します。
2. カスタムの役割を `.dat` ファイルにエクスポートするには、次の手順を実行します。このファイルは別の Apex One サーバに再度インポートできます。
   a. 役割を選択して、[エクスポート] > [DAT 形式でエクスポート] をクリックします。

b. .dat ファイルを保存します。別の Apex One サーバを管理している場合、.dat ファイルを使用して、カスタムの役割をそのサーバにインポートします。

注意

役割のエクスポートは、同じバージョンのサーバ間でのみ実行できます。

---

3. カスタムの役割を.csv ファイルにエクスポートするには

   a. 役割を選択して、[エクスポート] > [CSV 形式でエクスポート] をクリックします。

   b. .csv ファイルを保存します。このファイルを使用して、選択した役割に関する情報と権限を確認できます。

4. 他の Apex One サーバでカスタムの役割を保存し、その役割を現在の Apex One サーバにインポートする場合、[インポート] をクリックして、カスタムの役割が格納された.dat ファイルを選択します。

   - [ユーザの役割] 画面に表示される役割は、同じ名前の役割をインポートしたときに上書きされます。
   - 役割のインポートは、同じバージョンのサーバ間でのみ実行できます。
   - 他の Apex One サーバからインポートされた役割:
     - サーバ/エージェントのメニュー項目、および管理下のドメインのメニュー項目に対する権限は保持されます。
     - エージェント管理メニュー項目には初期設定の権限が適用されます。そのため、他のサーバ上でエージェント管理メニュー項目の役割の権限をメモに取り、インポートした役割に再適用する必要があります。

Trend Micro Apex Central

Trend Micro Apex Central™は、ゲートウェイ、メールサーバ、ファイルサーバ、および企業のデスクトップ向けの、トレンドマイクロ製品およびサービ

スを管理する中央管理コンソールです。Apex Central は Web ベースの管理コンソールであり、ネットワークを介して管理対象の製品およびサービスを一元的に監視できます。

システム管理者は Apex Central を使用して、感染、セキュリティ違反、ウイルスの侵入ポイントなどの処理を監視およびレポートできます。システム管理者は、ネットワークを介してコンポーネントをダウンロードおよび配信して、保護機能が一貫して最新に保たれるようにすることができます。Apex Central では手動または事前予約アップデートが可能で、グループとしてまたは個別に製品を設定および管理できることで柔軟性が加わります。

今回の Apex One リリースにおける Apex Central との統合

この Apex One のリリースには、Apex Central から Apex One サーバを管理するために次の機能が用意されています。

- Trend Micro Apex One ウイルス対策、情報漏えい対策、およびデバイスコントロール用のポリシーを作成、管理、および配信します。さらに Apex Central コンソールからセキュリティエージェントに権限を直接割り当てます。

  次の表は、Apex Central (すべてのバージョン) で使用可能なポリシー設定のリストを示しています。

表 14-15. Apex Central での Apex One のポリシー管理の種類

ポリシーの種類	機能
Apex One ウイルス対策およびエージェントの設定	• 追加サービス設定 • アプリケーションコントロール設定 • 挙動監視設定 • デバイスコントロール設定 • Endpoint Sensor 設定 • 手動検索設定 • 機械学習型検索の設定 • 権限とその他の設定 • リアルタイム検索設定 • サンプル送信 • 検索方法 • ScanNow 設定 • 予約検索設定 • スパイウェア/グレーウェアの承認済みリスト • 不審接続監視設定 • 信頼済みプログラムリスト • アップデートエージェント設定 • 仮想パッチ設定 • Web レピュテーション設定
情報漏えい対策オプション	情報漏えい対策ポリシー設定 **注意** 情報漏えい対策オプションのためのデバイスコントロール権限は、セキュリティエージェントのポリシーで管理します。

セキュリティエージェントのポリシー設定を Apex Central サーバに移行する作業の詳細については、603 ページの「Apex One 設定エクスポートツール」を参照してください。

- Apex Central コンソールを使用して、次の設定をある Trend Micro Apex One サーバから別の Apex One サーバに複製します。
  - 455 ページの「データ識別子の種類」
  - 469 ページの「情報漏えい対策テンプレート」

注意

情報漏えい対策オプションのライセンスがアクティベートされていない Trend Micro Apex One サーバに、これらの設定が複製された場合、その設定はライセンスがアクティベートされたときに有効になります。

Apex Central を介した高度な製品の統合

Apex Central Web コンソールでは、Apex One Web コンソールでは利用できない、高度なセキュリティエージェントポリシーの設定を利用できます。適切なライセンスを使用することで、ネットワークを介して次の高度なセキュリティポリシーをセキュリティエージェントに送信できます。

機能	説明
アプリケーションコントロール	アプリケーションコントロールとの統合により、Apex One ユーザは、高度なアプリケーションブロック機能とエンドポイントのロックダウン機能を利用できます。アプリケーション インベントリを実行し、一部のアプリケーションにのみエンドポイントでの実行を許可するポリシールールを作成することができます。アプリケーションのカテゴリ、ベンダ、またはバージョンに基づいてアプリケーションコントロールルールを作成することもできます。
Endpoint Sensor	Endpoint Sensor との統合により、Apex One エンドポイントに対して現在だけでなく過去のセキュリティ調査も監視、記録、実行できます。Root Cause Analysis を実施して攻撃を識別する前に、Apex Central 管理コンソールで事前診断に基づく調査を実施し、危険にさらされているエンドポイントを特定します。

機能	説明
仮想パッチ	仮想パッチとの統合により、パッチの正式リリース前に仮想パッチを自動で適用することで Apex One ユーザを保護します。トレンドマイクロは、ネットワークパフォーマンスとセキュリティの優先事項に基づいて、推奨される侵入防御ルールを保護対象のエンドポイントに提供します。

高度な製品の統合については、Apex Central の管理者ガイドを参照してください。

Trend Micro Apex Central

このバージョンの Apex One は、次のバージョンの Apex Central/Control Manager をサポートしています。

- Apex Central (すべてのバージョン)
- Control Manager 7.0 以降

Apex One サーバおよびセキュリティエージェントが Apex Central へのレポートに使用する IP アドレスの詳細については、812 ページの「IP アドレスが表示される画面」を参照してください。

これらの Apex Central のバージョンには最新の Patch および重要な HotFix を適用して、Apex Central で Apex One を管理できるようにしてください。最新の Patch と HotFix を入手するには、次のトレンドマイクロの最新版ダウンロードサイトにアクセスするか、サポート担当者にお問い合わせください。

http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

Apex One をインストールしたら、Apex Central に登録して Apex Central 管理コンソールで Apex One の設定を行います。Apex One サーバの管理については、Apex Central のドキュメントを参照してください。

Apex One の Apex Central への登録

手順

1. [管理] > [設定] > [Apex Central] に移動します。
2. エンティティ表示名を指定します。これは、Apex Central に表示される Apex One サーバの名前です。

   初期設定では、エンティティ表示名には、サーバコンピュータのホスト名とこの製品の名前が表示されます (例: Server01_OSCE)。

   注意

   Apex Central では、Apex Central によって管理される Apex One サーバやその他の製品を「エンティティ」と呼んでいます。
3. このサーバとの接続に使用される Apex Central サーバの FQDN または IP アドレスとポート番号を指定します。オプションで、HTTPS を使用して強化されたセキュリティに接続します。
   - デュアルスタックの Apex One サーバでは、Apex Central FQDN または IP アドレス (IPv4 か、IPv6 (使用可能な場合))を入力します。
   - IPv4 シングルスタックの Apex One サーバでは、Apex Central FQDN または IPv4 アドレスを入力します。
   - IPv6 シングルスタックの Apex One サーバでは、Apex Central FQDN または IPv6 アドレスを入力します。
4. [Apex Central 証明書] の横にある [参照] をクリックし、対象の Apex Central サーバからダウンロードした証明書ファイルを選択します。

   Apex Central 証明書ファイルを入手するには、Apex Central サーバに移動し、次の場所にある証明書ファイルを Apex One サーバにコピーします。

   ```
   <Apex Central のインストールフォルダ>¥Certificate¥CA
   ¥TMCM_CA_Cert.pem
   ```

   重要

   カスタマイズした証明書を Apex Central サーバで使用している場合は、Apex Central への登録時にルート CA 証明書をアップロードする必要があります。

詳細については、602 ページの「Apex Central 証明書の承認」を参照してください。

5. Apex Central の IIS Web サーバに認証が必要な場合、ユーザ名とパスワードを入力します。

6. プロキシサーバを使用して Apex Central サーバに接続する場合、次のプロキシ設定を指定します。

   - プロキシプロトコル
   - サーバ FQDN または IPv4/IPv6 アドレスおよびポート
   - プロキシサーバ認証用のユーザ ID とパスワード

7. ポート転送に一方向通信と双方向通信のどちらを使用するかを決定し、IPv4/IPv6 アドレスとポートを指定します。

8. Apex One が、指定した設定に基づいて Apex Central サーバに接続できるかどうかをチェックするには、[接続テスト] をクリックします。

   接続が正しく確立された場合は、[登録] をクリックします。

9. Control Manager サーバのバージョンが 6.0 SP1 以降の場合や Apex Central サーバを使用している場合、Apex Central サーバを Apex One 統合 Smart Protection Server のアップデート元として使用するかどうかを確認するメッセージが表示されます。Apex Central サーバを統合 Smart Protection Server のアップデート元として使用する場合は [OK] を、現在のアップデート元 (初期設定ではトレンドマイクロのアップデートサーバ) を引き続き使用する場合は [キャンセル] をクリックします。

10. 登録後にこの画面のいずれかの設定を変更した場合、設定を変更した後に [アップデート設定] をクリックして、Apex Central サーバに変更を通知します。

注意

Apex Central サーバが仮想アナライザに接続されている場合、登録完了後に自動登録プロセスが開始されます。詳細については、608 ページの「不審オブジェクトリスト設定」を参照してください。

11. Apex Central サーバで Apex One を管理しないようにする場合、[登録取り消し] をクリックします。

Apex Central 証明書の承認

Apex One を Apex Central サーバに登録する前に、Apex Central 証明書ファイルを Apex Central サーバの次の場所から入手する必要があります。

`<Apex Central のインストールフォルダ>¥Certificate¥CA ¥TMCM_CA_Cert.pem`

Apex One と Apex Central では、この証明書と公開鍵暗号化を使用して、登録やポリシー管理において承認されたサーバ間での通信のみを許可します。どちらかのサーバが不正な通信を検出すると、受信中の登録またはポリシー設定はすべて拒否されます。

重要

カスタマイズした証明書を Apex Central サーバで使用している場合は、Apex Central への登録時にルート CA 証明書をアップロードする必要があります。

Apex Central 管理コンソールでの Apex One の状態の確認

手順

1. Apex Central 管理コンソールを開きます。

   Apex Central コンソールを開くには、ネットワーク上の任意のエンドポイントで Web ブラウザを開き、次の URL を入力します。

   `https://<Apex Central のサーバ名>/Webapp/login.aspx`

   ここで、`<Apex Central のサーバ名>` は Apex Central サーバの IP アドレスまたはホスト名です。

2. メインメニューで、[ディレクトリ] > [製品] の順にクリックします。

3. 表示されたツリーで、[<Apex Central のサーバ名>] > [ローカルフォルダ] > [新規エンティティ] の順にフォルダを展開します。

4. Apex One サーバのアイコンが表示されているかどうかを確認します。

Apex One 設定エクスポートツール

Apex One では Apex One 設定エクスポートツールが提供されており、管理者は Apex One の設定を前のバージョンのウイルスバスター Corp.から現在のバージョンにコピーすることができます。Apex One 設定エクスポートツールにより、次の設定を移行できます。

機能	移行される設定
[エージェント管理] **注意** Apex One 設定エクスポートツールは、適用可能なエージェント管理設定を ApexOne_Agent_DLP_Policies.zip パッケージと ApexOne_Agent_Policies.zip パッケージに移行して、Apex Central へのインポート時に使用できるようにします。	• 手動検索 • 予約検索 • リアルタイム検索 • ScanNow • 検索方法 • Web レピュテーション • 挙動監視 • デバイスコントロール • 情報漏えい対策 • 権限とその他の設定 • 追加サービス設定 • スパイウェア/グレーウェアの承認済みリスト • 機械学習型検索 • 不審接続監視 • 信頼済みプログラムリスト **注意** • 手動検索、予約検索、リアルタイム検索、および ScanNow のバックアップディレクトリは移行されません。 • 設定は、ルートおよびドメインレベルの両方で保持されます。

機能	移行される設定
エージェントのグループ設定	すべての設定 **注意** Active Directory との初回同期後に、Active Directory ドメインの構造が表示されます。
グローバルエージェント設定	すべての設定
エンドポイントの位置	• 位置認識設定 • ゲートウェイ IP アドレスおよび MAC のリスト
情報漏えい対策	• データ識別子 • テンプレート
ファイアウォール	• ポリシー • プロファイル
ログ管理	すべての設定
エージェントアップデート元	• エージェントアップデート元 • ユーザアップデート元リスト
Smart Protection ソース	ユーザ指定 Smart Protection ソースリスト
通知	• 一般通知設定 • 管理者通知設定 • アウトブレーク通知設定 • エージェント通知設定
プロキシ	すべての設定
オフラインエージェント	すべての設定
隔離フォルダ	すべての設定

機能	移行される設定
Web コンソール	すべての設定
ofcscan.ini の設定	• [INI_CLIENT_INSTALLPATH_SECTION] WinNT_InstallPath • [INI_REESTABLISH_COMMUNICATION_SECTION]: すべての設定
ofcserver.ini の設定	[INI_SERVER_DISK_THRESHOLD]: すべての設定

注意

- ウイルスバスター Corp.サーバのセキュリティエージェントリストはバックアップされず、ドメイン構造のみがバックアップされます。
- このツールは、古いバージョンのウイルスバスター Corp.サーバで利用可能な機能のみ移行します。古いサーバで使用できない機能については、初期設定が適用されます。

Apex One 設定エクスポートツールの使用

注意

このバージョンの Apex One は、次の移行をサポートしています。

- オンプレミスの Apex One サーバ: ウイルスバスター Corp. 11.0 以降からの移行
- Apex One as a Service サーバ: ウイルスバスター Corp. XG Service Pack 1 からの移行

Apex One 設定エクスポートツールによって移行される設定の一覧については、603 ページの「Apex One 設定エクスポートツール」を参照してください。

古いバージョンのウイルスバスター Corp.には、最新バージョンの Apex One で利用可能な設定がすべて含まれていない可能性があります。Apex One は、前のバージョンのウイルスバスター Corp.サーバから移行されていない機能には自動的に初期設定を適用します。

手順

1. サーバ移行ツールのパッケージを探します。

   - Apex One Web コンソールで、[管理] > [設定] > [サーバの移行] に移動し、[Apex One 設定エクスポートツールのダウンロード] リンクをクリックします。
   - Apex One サーバコンピュータで、<サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility¥PolicyExportTool に移動します。

2. Apex One 設定エクスポートツールをエクスポート元のウイルスバスター Corp.サーバコンピュータにコピーします。

   重要

   すべてのデータが移行先サーバに対して正しくフォーマットされるように、エクスポート元のウイルスバスター Corp.サーバで Apex One 設定エクスポートツールを使用する必要があります。Apex One は、古いバージョンのサーバ移行ツールには対応していません。

3. 管理権限を使用してコマンドプロンプトを開き、ツールの場所に移動して、ApexOneSettingsExportTool.exe を実行します。

   Apex One 設定エクスポートツールが実行されます。

   注意

   エクスポートパッケージの初期設定の名前は次のとおりです。

   - ApexOne_Agent_DLP_Policies.zip (情報漏えい対策ポリシー設定を Apex Central にインポートする際に使用)
   - ApexOne_Agent_Policies.zip (セキュリティエージェントのその他すべてのポリシー設定を Apex Central にインポートする際に使用)
   - Server_Settings_Migration.zip (セキュリティエージェントのすべてのポリシー設定およびウイルスバスター Corp.サーバの設定を、別の Apex One サーバにインポートする際に使用)

4. エクスポートパッケージを、エクスポート先の Apex One サーバまたは Apex Central サーバがアクセスできる場所にコピーします。

5. エクスポート先の Apex One サーバに設定をインポートするには

   a. Apex One Web コンソールで、[管理] > [設定] > [サーバの移行] に移動し、[設定のインポート...] ボタンをクリックします。

   b. `Server_Settings_Migration.zip` パッケージを探し、[開く] をクリックします。

   c. サーバに前のバージョンのウイルスバスター Corp.の設定がすべて含まれていることを確認します。

6. エクスポート先の Apex Central コンソールにセキュリティエージェントのポリシー設定をインポートするには

   a. Apex Central Web コンソールで、[ポリシー] > [ポリシー管理] に移動します。

   b. [製品] のドロップダウンで、[Apex One セキュリティエージェント] を選択します。

   c. [設定のインポート] をクリックします。

   d. `ApexOne_Agent_Policies.zip` パッケージを探し、[開く] をクリックします。

7. エクスポート先の Apex Central コンソールにセキュリティエージェントの情報漏えい対策ポリシー設定をインポートするには

   a. Apex Central Web コンソールで、[ポリシー] > [ポリシー管理] に移動します。

   b. [製品] のドロップダウンで、[Apex One 情報漏えい対策] を選択します。

   c. [設定のインポート] をクリックします。

   d. `ApexOne_Agent_DLP_Policies.zip` パッケージを探し、[開く] をクリックします。

8. 古いセキュリティエージェントを新しい Apex One サーバに移動します。

セキュリティエージェントの移動の詳細については、81 ページの「別のドメインまたはサーバへのセキュリティエージェントの移動」または 660 ページの「エージェント移動ツール」を参照してください。

不審オブジェクトリスト設定

不審オブジェクトとは、Deep Discovery 製品やその他のソースによる分析によって危険な可能性があると判断されたデジタル情報です。Apex One では、不審オブジェクトを Deep Discovery に接続されている Control Manager 7.0 (以降) または Apex Central 2019 (以降) のサーバと同期して、対応する処理を取得します。

Control Manager または Apex Central に登録した後、ネットワーク上のエージェントで検出された C&C コールバックまたはターゲット攻撃を監視する不審オブジェクトの種類を選択します。不審オブジェクトには次の種類があります。

- 不審 URL リスト
- 不審 IP リスト
- 不審ファイルリスト
- 不審ドメインリスト

注意

Apex One が Deep Discovery Analyzer に登録されている場合は、有効にできるのは不審 URL リストだけです。Deep Discovery Analyzer への登録を解除した後に、再度登録することはできません。不審オブジェクトを同期するには、Deep Discovery に接続されている Apex Central に登録する必要があります。

Apex Central での不審オブジェクトの管理方法については、Apex Central の管理者ガイドを参照してください。

不審オブジェクトリストの設定

オンプレミスの Apex Central に Apex One を登録するための API キーが Apex One に配信されます。この自動登録プロセスが実行されるようにする

には、Apex Central が仮想アナライザに接続されているか、不審オブジェクトリストが手動で設定されていることを Apex Central 管理者に確認してください。

Apex Central サーバへの登録の詳細については、599 ページの「Apex One の Apex Central への登録」を参照してください。

手順

1. [管理] > [設定] > [不審オブジェクトリスト] に移動します。
2. エージェントで有効にするリストを選択します。
   - 不審 URL リストを有効にする
   - 不審 IP リストを有効にする (登録済み Apex Central サーバまたは Control Manager サーバに登録する場合にのみ使用可能)
   - 不審ファイルリストを有効にする (登録済み Apex Central サーバまたは Control Manager サーバに登録する場合にのみ使用可能)
   - 不審ドメインリストを有効にする (登録済み Apex Central サーバまたは Control Manager サーバに登録する場合にのみ使用可能)

   管理者は、[今すぐ同期] ボタンをクリックすることで、いつでも不審オブジェクトリストを手動で同期できます。
3. [セキュリティエージェントの不審オブジェクトリストのアップデート] で、エージェントで不審オブジェクトリストをアップデートするタイミングを指定します。
   - セキュリティエージェントのコンポーネントのアップデートスケジュールに従う: 現在のアップデートスケジュールに従って不審オブジェクトリストがアップデートされます。
   - サーバで不審オブジェクトリストがアップデートされたときに自動的に実行する: サーバがアップデートされたリストを受信したときに自動的に不審オブジェクトリストがアップデートされます。

注意

アップデートエージェントからアップデートを受信するように設定されていないセキュリティエージェントでは、同期時に登録済み不審オブジェクトリストの差分アップデートが実行されます。

4. [保存]をクリックします。

参照サーバ

セキュリティエージェントでどのポリシーまたはプロファイルを使用するかを決定する方法の 1 つは、Apex One サーバとの接続状態をチェックすることです。内部セキュリティエージェント (企業のネットワーク内のエージェント) がサーバに接続できない場合、エージェントの状態はオフラインになります。この場合、このエージェントには、外部エージェント用のポリシーまたはプロファイルが適用されます。この問題に対処するのが参照サーバです。

Apex One サーバとの接続が切断されたセキュリティエージェントは、参照サーバとの接続を試行します。エージェントが参照サーバとの接続の確立に成功すると、内部エージェント用のポリシーまたはプロファイルが適用されます。

参照サーバにより管理されるポリシーおよびプロファイルは、次のとおりです。

- ファイアウォールプロファイル
- Web レピュテーションポリシー
- 情報漏えい対策オプションポリシー
- デバイスコントロールポリシー

次の点に注意してください。

- サーバの機能 (Web サーバ、SQL サーバ、FTP サーバなど) を持つコンピュータを、参照サーバとして割り当てます。最大 320 の参照サーバを指定できます。

- セキュリティエージェントは、参照サーバリスト上の 1 番目の参照サーバに接続します。接続が確立できない場合、エージェントはリスト上の 2 番目のサーバへの接続を試行します。
- セキュリティエージェントは、使用するウイルス対策 (挙動監視、デバイスコントロール、ファイアウォールプロファイル、Web レピュテーションポリシー) または情報漏えい対策オプション設定を決定する際に参照サーバを使用します。参照サーバでは、エージェントを管理したり、アップデートやエージェント設定を配信することはありません。このようなタスクは、Apex One サーバが実行します。
- セキュリティエージェントは、ログを参照サーバに送信したり、参照サーバをアップデート元として使用することはできません。

参照サーバリストの管理

手順

1. [エージェント] > [ファイアウォール] > [プロファイル] または [エージェント] > [エンドポイントの位置] に移動します。
2. 表示される画面に応じて、次の操作を実行します。
   - [エージェントのファイアウォールプロファイル] 画面を表示している場合は、[参照サーバリストの編集] をクリックします。
   - [エンドポイントの位置] 画面を表示している場合は、[参照サーバリスト] をクリックします。
3. [参照サーバリストを有効にする] を選択します。
   - VPN または PPP ダイヤルアップ接続を使用するエージェントを除外する: 参照サーバへの接続に VPN または PPP (ポイントツーポイントプロトコル) ダイヤルアップ接続を使用するエンドポイントを外部エージェントとして定義する場合に選択します。
4. リストにエンドポイントを追加するには、[追加] をクリックします。
   a. 次のように、エンドポイントの Pv4/IPv6 アドレス、名前、または完全修飾ドメイン名 (FQDN) を指定します。

- `computer.networkname`
- `12.10.10.10`
- `mycomputer.domain.com`

b. エージェントがこのエンドポイントとの通信に使用するポートを入力します。参照サーバで開いている任意の接続ポート (ポート 20、23、80 など) を指定します。

> **注意**
>
> 同じ参照サーバに別のポート番号を指定するには、手順 2a と 2b を繰り返します。セキュリティエージェントはリスト上の 1 番目のポート番号を使用し、接続に失敗すると、2 番目のポート番号を使用します。

c. [保存] をクリックします。

5. リストのエンドポイントの設定を修正するには、エンドポイント名をクリックします。エンドポイント名またはポートを変更して、[保存] をクリックします。
6. エンドポイントをリストから削除するには、エンドポイント名を選択して [削除] をクリックします。
7. エンドポイントが参照サーバとして機能するようにするには、[エージェントに割り当てる] をクリックします。

管理者通知設定

Apex One がメールおよび SNMP トラップで通知を正常に送信できるように、管理者通知設定を行ってください。Apex One では、Windows NT イベントログを使用しても通知を送信できますが、この通知チャネルに対して実行される設定はありません。

Apex One では、次の検出時に、それぞれの Apex One 管理者に通知を送信できます。

表 14-16. 管理者への通知を実行する検出

検出内容	通知チャネル		
	メール	SNMP トラップ	WINDOWS NT イベントログ
ウイルスと不正プログラム	あり	あり	あり
スパイウェアとグレーウェア	あり	あり	あり
デジタル資産の転送	あり	あり	あり
C&C コールバック	あり	あり	あり
ウイルスと不正プログラムの大規模感染	あり	あり	あり
スパイウェアとグレーウェアの大規模感染	あり	あり	あり
ファイアウォール違反アウトブレーク	あり	なし	なし
共有フォルダセッションの大規模感染	あり	なし	なし
C&C コールバックアウトブレーク	あり	あり	あり

一般通知

手順

1. [管理] > [通知] > [一般設定] に移動します。
2. メール通知を設定します。
   a. [SMTP サーバ] に、SMTP サーバのエンドポイント名か、IPv4/IPv6 アドレスのいずれかを指定します。
   b. SMTP サーバで使用するポートを指定します。

      有効なポート番号は 1～65535 です。

c. [送信者] に、通知の送信者として表示するメールアドレスを指定します。

次の手順で ESMTP を有効化する場合は、有効なメールアドレスを指定します。

d. 必要に応じて、[ESMTP を有効にする] をクリックします。

e. [送信者] フィールドに、指定したメールアドレスのユーザ名とパスワードを指定します。

f. サーバに対してエージェントを認証する方法を選択します。

- ログイン: ログインは、古いバージョンのメールユーザエージェントです。サーバとエージェントは両方とも、BASE64 を使用してユーザ名とパスワードを認証します。
- プレーンテキスト: プレーンテキストは最も簡単に使用できる方法ですが、ユーザ名とパスワードが BASE64 でエンコードされた 1 つの文字列としてインターネット経由で送信されるため、安全でない場合もあります。
- CRAM-MD5: CRAM-MD5 では、チャレンジレスポンス方式の認証メカニズムと暗号化メッセージダイジェスト 5 アルゴリズムを組み合わせて使用し、情報の交換と認証を行います。
- NTLM: NTLM 認証では、チャレンジ/レスポンス方式のメカニズムを使用して、ユーザがサーバに対して、入力したパスワードがユーザアカウントに適切であることを証明できるようにします。

  [SSL/TLS 暗号化を使用する] を有効にして、NTLM 認証をさらに暗号化します。

3. SNMP トラップ通知を設定します。

a. [サーバ IP アドレス] に IPv4/IPv6 アドレスか、エンドポイント名のいずれかを指定します。

b. コミュニティ名には、推測しにくいものを指定してください。

注意

セキュリティ上の理由から、コミュニティ名の値はアスタリスク (*) 文字でマスクされて表示されます。初期設定の値は「public」です。

4. [保存] をクリックします。

システムイベントログ

Apex One では、起動や終了などのサーバプログラムに関するイベントを記録します。これらのログを使用して、Apex One サーバおよびサービスが適切に稼働していることを確認します。

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログの削除スケジュールを設定します。ログの管理方法の詳細については、616 ページの「ログ管理」を参照してください。

システムイベントログの表示

手順

1. [ログ] > [システムイベント]に移動します。
2. [イベント] で、詳細な処理が必要なログを確認します。Apex One では次のイベントをログに記録します。

表 14-17. システムイベントログ

検索の種類	イベント
Apex One マスターサービスおよびデータベースサーバ	• マスターサービスの起動 • マスターサービスの正常停止 • マスターサービスの異常停止

検索の種類	イベント
大規模感染予防サービス	• 大規模感染予防サービスの有効化 • 大規模感染予防サービスの無効化 • 最後の <number of minutes> 分の共有フォルダセッションの数
データベースバックアップ	• データベースバックアップの成功 • データベースバックアップの失敗
役割ベースの Web コンソールのアクセス	• コンソールへのログオン • パスワードの変更 • コンソールからのログオフ • セッションタイムアウト (ユーザは自動的にログオフされます)
サーバ認証	• セキュリティエージェントがサーバから無効なコマンドを受信した • 認証証明書が無効または期限切れ
仮想アナライザ	• 分析用のサンプルの送信 • サンプルの分析の完了 • 仮想アナライザが、接続されている別の Apex One サーバからの前回の重複するサンプル送信を報告した

3. ログを CSV ファイルに保存するには、[CSV 形式でエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。

ログ管理

Apex One では、セキュリティリスクの検出、イベント、およびアップデートに関する包括的なログを保持します。これらのログを使用して、組織の保護ポリシーを評価し、感染や攻撃のリスクが高いセキュリティエージェントを特定します。また、これらのログは、エージェントとサーバ間の接続のチェッ

ク、およびコンポーネントのアップデートが成功したかどうかの確認にも使用できます。

Apex One では、サーバ側からの確認メカニズムを使用して、Apex One サーバとエージェントの間の時刻の一貫性を確保することもできます。タイムゾーン、夏時間、および時差によってログの不一致が発生すると、ログの分析時に混乱を引き起こす可能性がありますが、このメカニズムを利用することでそれを回避できます。

注意

サーバアップデートログおよびシステムイベントログを除くすべてのログに対して時間が確認されます。

Apex One サーバがセキュリティエージェントから受信するログは次のとおりです。

- 362 ページの「ウイルス/不正プログラムログの表示」
- 370 ページの「スパイウェア/グレーウェアログの表示」
- 375 ページの「スパイウェア/グレーウェア復元ログの表示」
- 564 ページの「ファイアウォールログの表示」
- 533 ページの「Web レピュテーションログの表示」
- 404 ページの「不審接続監視ログの表示」
- 375 ページの「不審ファイルログの表示」
- 534 ページの「C&C コールバックログの表示」
- 428 ページの「挙動監視ログの表示」
- 401 ページの「機械学習型検索ログの表示」
- 448 ページの「デバイスコントロールログの表示」
- 376 ページの「検索ログの表示」
- 506 ページの「情報漏えい対策ログの表示」

- 256 ページの「セキュリティエージェントアップデートログの表示」
- 681 ページの「接続状態の確認ログの表示」

Apex One サーバでは次のログを生成します。

- 230 ページの「Apex One サーバのアップデートログ」
- 615 ページの「システムイベントログ」

Apex One サーバおよびセキュリティエージェントでは、次のログも使用できます。

- 796 ページの「Windows イベントログ」
- 777 ページの「Apex One サーバログ」
- 787 ページの「セキュリティエージェントログ」

ログ管理

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、Web コンソールで手動でログを削除するか、またはログの削除スケジュールを設定します。

スケジュールに基づくログの削除

手順

1. [ログ] > [ログ管理] に移動します。
2. [ログの自動削除を有効にする] を選択します。
3. 削除するログタイプを選択します。Apex One で生成されるログは、デバッグログ以外のすべてのログを予約に基づいて削除できます。デバッグログの場合、デバッグログを無効にしてログの収集を停止します。

注意

ウイルス/不正プログラムログの場合、特定の検索の種類やダメージクリーンナップサービスで生成されたログを削除できます。スパイウェア/グレーウェアログの場合、特定の検索の種類のログを削除できます。検索の種類の詳細については、285 ページの「検索の種類」を参照してください。

4. 選択したすべてのログタイプのログを削除するか、特定の日数より古いログのみを削除するかを選択します。
5. ログを削除する頻度と時刻を指定します。
6. [保存] をクリックします。

ログの手動削除

手順

1. [ログ] > [エージェント] > [セキュリティリスク] または [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. 次の手順のいずれかを実行します。
   - [セキュリティリスクログ] 画面を表示している場合は、[ログの削除] をクリックします。
   - [エージェント管理] 画面を表示している場合は、[ログ] > [ログの削除] をクリックします。
4. [削除するログタイプ] で、削除するログデータのタイプを選択します。
   - 挙動監視ログ
   - C&C コールバックログ
   - 情報漏えい対策ログ

- デバイスコントロールログ
- ファイアウォールログ
- 機械学習型検索ログ
- スパイウェア/グレーウェアログ
- 検索ログ
- 不審接続監視ログ
- 不審ファイルログ
- ウイルス/不正プログラムログ
- Web レピュテーションログ

注意

ウイルス/不正プログラムログの場合、特定の検索の種類やダメージクリーンナップサービスで生成されたログを削除できます。スパイウェア/グレーウェアログの場合、特定の検索の種類のログを削除できます。

検索の種類の詳細については、285 ページの「検索の種類」を参照してください。

5. [削除するログ] で、次のいずれかを選択します。
   - 選択したログタイプのすべてのログ: 選択したログタイプのすべてのログデータを削除します。
   - 次の期間を経過したログ: 選択したログタイプについて指定された日数より古いログデータをすべて削除します。
6. [削除] をクリックします。

ライセンス

Apex One のライセンス情報の表示、アクティベート、およびサポート契約の更新には、Web コンソールを使用します。

注意

情報漏えい対策オプション、Trend Micro VDI オプションなど Apex One のデフォルトの機能のいくつかには専用のライセンスが必要です。このような機能のライセンスは、プラグインマネージャからアクティベートと管理を行います。これらの機能のライセンスの詳細については、86 ページの「情報漏えい対策オプションライセンス」および 715 ページの「Trend Micro VDI オプションのライセンス」を参照してください。

IPv6 シングルスタックの Apex One サーバは、トレンドマイクロのオンライン登録サーバに接続してライセンスのアクティベート/サポート契約の更新を行うことができません。この Apex One サーバから登録サーバに接続するには、IP アドレスを変換可能な DeleGate などのデュアルスタックプロキシサーバが必要です。

ライセンス情報の管理

[ライセンス情報] 画面で、既存の製品ライセンスの詳細の確認や更新を行うことができます。

手順

1. [管理] > [設定] > [製品ライセンス]に移動します。
2. ライセンス情報を表示します。

項目	説明
製品	製品ライセンスの名前
ステータス	現在のライセンスのステータス
種類	製品版と体験版のいずれであるか
有効期限	ライセンスの有効期限
アクティベーションコード	トレンドマイクロに登録されている現在のアクティベーションコード
前回のアップデート	アップデートされたライセンス情報をトレンドマイクロサーバから最後に取得した時刻

3. 有効期限切れや有効期限が近いライセンスを更新します。

   a. [アクティベーションコードの指定]をクリックします。

      [新しいアクティベーションコード] 画面が表示されます。

   b. [アクティベーションコード] に新しいコードを貼り付けるか入力します。

   c. [保存] をクリックします。

      [ライセンス情報] 画面にアップデートされたライセンス情報が表示されます。

SQL Server データベース接続設定

SQL Server データベース設定ツールを使用して、Apex One サーバを既存の別の Apex One SQL データベースに接続したり、既存のデータベースへの接続に使用するログオン情報を変更したりできます。

SQL Server データベース設定ツールでは次の作業を実行できます。

- 既存の別の Apex One SQL Server データベースインスタンスに切り替える
- 既存の SQL Server データベースへのログオン情報を更新する
- SQL Server データベースが利用できなくなったときのアラートを設定する

SQL Server データベース接続の設定

SQL Server データベース設定ツールを使用して、Apex One サーバを既存の別の Apex One SQL データベースに接続したり、既存のデータベースへの接続に使用するログオン情報を変更したりできます。

手順

1. Apex One サーバコンピュータで、<サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility¥SQL に移動します。
2. SQLTxfr.exe をダブルクリックして、ツールを実行します。

   Apex One SQL Server データベース設定のコンソールが開きます。
3. [サーバ名] を次の形式で指定します。<SQL Server のホスト名または IP アドレス>,<ポート番号>\<インスタンス名>

   重要

   SQL Server をインストールすると、Apex One データベースのインスタンスが自動的に作成されます。既存の SQL Server またはデータベースに移行するときは、その SQL Server の既存の Apex One インスタンスの名前を入力してください。
4. SQL Server データベースの認証アカウント情報を指定します。
   - Windows アカウントを使用してサーバにログオンするときは、Apex One に現在ログオンしているユーザのユーザ名が適用されます。

     重要

     ユーザアカウントは、ローカル管理者グループに属しているか、Active Directory (AD) ビルトイン管理者である必要があります。また、Windows のローカルセキュリティポリシーまたはグループポリシー管理コンソールを使用して、次のユーザ権限割り当てポリシーを設定する必要があります。

     - サービスとしてログオン
     - バッチジョブとしてログオン
     - ローカルログオンを許可

     ユーザアカウントには、次に示すデータベースの役割も必要です。

     - dbcreator
     - bulkadmin
     - db_owner

5. [データベース名] セクションで、SQL Server 上の Apex One データベース名を指定します。
6. インストール中に Endpoint Sensor データベースを設定した場合は、Endpoint Sensor データベース名を指定します。

   注意

   Apex One データベースとは別の SQL インスタンスに Endpoint Sensor データベースがある場合は、データベースの管理方法に関する次の製品 Q&A の記事を参照してください。

   https://success.trendmicro.com/solution/1122929

7. 必要に応じて、次のタスクを実行します。
   - [Apex One データベース利用不可アラート...] をクリックして、Apex One SQL データベースの通知を設定します。

     詳細については、624 ページの「Apex One データベース利用不可アラートの設定」を参照してください。
   - [接続テスト] をクリックして、既存の SQL Server またはデータベースの認証アカウント情報を確認します。
8. [開始] をクリックして、設定変更を適用します。

Apex One データベース利用不可アラートの設定

Apex One は、SQL データベースが利用できなくなったときにこのアラートを自動的に送信します。

警告!

データベースが利用できなくなると、Apex One ではすべてのサービスが自動的に停止します。データベースが利用できない場合、エージェント情報やイベント情報のログへの記録、アップデートの実行、およびエージェントの設定を実行できません。

データベース利用不可アラートは、Apex One サーバデータベースのみに適用できますが、Endpoint Sensor データベースには適用されません。

手順

1. Apex One サーバコンピュータで、<サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility¥SQL に移動します。
2. SQLTxfr.exe をダブルクリックして、ツールを実行します。

   Apex One SQL Server データベース設定のコンソールが開きます。
3. [Apex One データベース利用不可アラート...] をクリックします。

   [Apex One データベース利用不可アラート] 画面が表示されます。
4. アラートの受信者のメールアドレスを入力します。

   複数のエントリを区切るには、セミコロン (;) を使用します。
5. 必要に応じて [件名] および [メッセージ] を変更します。

   Apex One では、次のトークン変数を使用できます。

   表 14-18. Apex One データベース利用不可アラートのトークン

変数	説明
%x	Apex One SQL Server インスタンスの名前
%s	影響を受ける Apex One サーバの名前

6. [OK] をクリックします。

Apex One Web サーバ/エージェント接続設定

Apex One サーバのインストール時に、Web サーバの設定が自動的に行われます。これにより、ネットワーク上のコンピュータが Apex One サーバに接続できるようになります。ネットワーク上のエンドポイントエージェントが接続する Web サーバを設定します。

Web サーバの設定を外部から (たとえば、IIS 管理コンソールから) 変更する場合、Apex One で変更を複製します。たとえば、ネットワーク上のコンピュータが接続するサーバの IP アドレスを手動で変更した場合、または動的 IP ア

ドレスを割り当てる場合、Apex One のサーバ設定を再設定する必要があります。

警告!

接続設定を変更すると、サーバとエージェントの間の接続が永続的に失われ、セキュリティエージェントの再配信が必要になる場合があります。

接続設定

手順

1. [管理] > [設定] > [エージェント接続] に移動します。
2. Web サーバのドメイン名または IPv4/IPv6 アドレスおよびポート番号を入力します。

   注意

   ポート番号は、Apex One サーバがセキュリティエージェントとの通信に使用する信頼されたポートです。
3. [保存] をクリックします。

サーバ/エージェント間通信

サーバとエージェント間のすべての通信が有効になるように Apex One を設定できます。Apex One では、公開鍵暗号法と高度な暗号化機能を使用して、サーバとエージェントの間のすべての通信を保護できます

通信の保護機能の詳細については、以下を参照してください。

- 627 ページの「サーバとエージェント間の認証」
- 630 ページの「サーバ/エージェント間通信の暗号化の強化」

サーバとエージェント間の認証

Apex One では、公開鍵暗号法を使用して、Apex One サーバからエージェントへの通信を認証します。公開鍵暗号法では、サーバは秘密鍵を保持し、すべてのエージェントに公開鍵を配布します。エージェントは、公開鍵を使用して、受信する通信がサーバから開始された有効なものかどうかを検証します。検証に成功した場合、エージェントは応答します。

注意

Apex One では、エージェントからサーバへの通信は、サーバ側では認証されません。

公開鍵と秘密鍵は、トレンドマイクロの証明書に関連付けられています。Apex One サーバのインストール時、ホストの証明書ストアにこの証明書が格納されます。トレンドマイクロの証明書および鍵を管理するには、認証証明書マネージャツールを使用します。

すべての Apex One サーバで同じ認証鍵を使用するかどうかは、次の点に考慮して判断します。

- 1 つの証明書鍵を実装する方法は、標準レベルのセキュリティで広く採用されています。組織のセキュリティをある程度維持しつつ、複数の鍵を管理する手間を軽減できます。
- Apex One サーバごとに証明書鍵を実装すると、より安全性が高くなります。ただし、証明書鍵を再配布する必要が生じた場合は管理作業が増加します。

重要

Apex One サーバを再インストールする前に、必ず既存の証明書をバックアップしてください。新しいインストールの完了後、バックアップした証明書をインポートし、Apex One サーバとセキュリティエージェント間の通信認証が中断されないようにします。サーバのインストール時に新しい証明書を作成した場合は、セキュリティエージェントは (すでに存在しない) 古い証明書を引き続き使用しているため、サーバ通信を認証できません。

証明書のバックアップ、復元、エクスポート、およびインポートの詳細については、628 ページの「認証証明書マネージャの使用」を参照してください。

認証証明書マネージャの使用

Apex One サーバは、期限切れの公開鍵を持つセキュリティエージェントのために期限切れの証明書を保持しています。たとえば、長期間サーバに接続していないセキュリティエージェントの公開鍵は期限切れになっています。このようなセキュリティエージェントは、再接続時、サーバ開始通信を認識できるように期限切れの公開鍵を期限切れの証明書に関連付けます。その後、サーバは最新の公開鍵をセキュリティエージェントに配信します。

証明書を設定するときは、次の点に注意してください。

- 証明書パスには、マップされたドライブおよび UNC パスを使用できます。
- 強力なパスワードを指定し、後で確認できるように控えてください。

重要

認証証明書マネージャツールを使用するときは、次の要件に注意してください。

- ユーザには管理者権限がある必要があります。
- このツールで管理できるのはローカルエンドポイントにある証明書だけです。

手順

1. Apex One サーバで、コマンドプロンプトを開き、ディレクトリを<サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility¥CertificateManager に変更します。
2. 以下のコマンドのいずれかを実行します。

コマンド	例	説明
CertificateManager.exe -c [バックアップパスワード]	CertificateManager.exe -c strongpassword	新しいトレンドマイクロの証明書を生成し、既存の証明書と置き換えます。 このコマンドは、既存の証明書が期限切れになっている場合や、権限のないユーザに漏えいした場合に実行してください。

コマンド	例	説明
CertificateManager.exe -r [パスワード] [証明書パス] **注意** 証明書は ZIP 形式です。	CertificateManager.exe -r strongpassword D:\Test\TrendMicro.zip	サーバでトレンドマイクロの証明書をすべて復元し、証明書のプロパティをエクスポート可能として設定します。 このコマンドは、再インストールした Apex One サーバで証明書を復元する場合に実行してください。
CertificateManager.exe -re [パスワード] [証明書パス] **注意** 証明書は ZIP 形式です。	CertificateManager.exe -re strongpassword D:\Test\TrendMicro.zip	サーバでトレンドマイクロの証明書をすべて復元し、証明書のプロパティをエクスポート不可として設定します。 このコマンドは、再インストールした Apex One サーバで証明書を復元する場合に実行してください。
CertificateManager.exe -e [証明書パス]	CertificateManager.exe -e <エージェントインストールフォルダ>\OfcNTCer.dat	現在使用されている証明書に関連付けられたセキュリティエージェントの公開鍵をエクスポートします。 このコマンドは、エンドポイントで使用している公開鍵が破損した場合に実行してください。.dat ファイルをエンドポイントのルートフォルダにコピーして、既存のファイルを上書きしてください。 **重要** セキュリティエージェントの証明書のファイルパスは、次の形式にする必要があります。 <エージェントインストールフォルダ>¥OfcNTCer.dat

コマンド	例	説明
CertificateManager.exe -ine [パスワード] [証明書パス] 注意 初期設定での証明書のファイル名: OfcNTCer.pfx	CertificateManager.exe -ine strongpassword D:\Test\OfcNTCer.pfx	トレンドマイクロの証明書を証明書ストアにインポートします。 重要 ine コマンドを実行すると、証明書がインポートされ、証明書のプロパティが自動でエクスポート不可に設定されます。
CertificateManager.exe -l [CSV パス]	CertificateManager.exe -l D:\Test\MismatchedAgentList.csv	一致しない証明書を現在使用しているエンドポイントをリストします (CSV 形式)。

サーバ/エージェント間通信の暗号化の強化

Apex One の暗号化機能が強化され、サーバとエージェント間の通信に AES (Advanced Encryption Standard) 256 暗号化を使用して公的なコンプライアンス標準に対応できるようになりました。

重要

Apex One では、AES-256 暗号化はウイルスバスター Corp. 11.0 SP1 以降およびプラグインマネージャ 2.2 以降を実行しているサーバおよびエージェントでのみサポートされます。

警告!

AES-256 暗号化を有効にする前に、サーバの管理対象となるすべてのエージェントをバージョン 11.0 SP1 にバージョンアップしてください。古いバージョンのエージェントでは、AES-256 で暗号化された通信を復号できない可能性があります。古いバージョンのエージェントで AES-256 暗号化を有効にすると、プロキシサーバの使用時に Apex One サーバとの通信が完全に失われる可能性があります。

手順

1. [エージェント] > [グローバルエージェント設定]に移動します。
2. [ネットワーク] タブをクリックします。
3. [サーバ/エージェント間通信] セクションに移動します。
4. [Apex One サーバ/セキュリティエージェント間通信の AES-256 暗号化] の横の [変更] ボタンをクリックします。

   メッセージが表示されます。
5. [バージョンの確認] をクリックして、すべてのエージェントがウイルスバスター Corp. 11.0 SP1 以降にバージョンアップされたことを確認します。
6. [OK] をクリックします。

Web コンソールパスワード

Web コンソールのパスワード (または Apex One サーバのインストール時に作成したルートアカウントのパスワード) を管理する画面は、役割ベースの管理を使用するのに必要な環境がサーバコンピュータにない場合にのみアクセスできます。リソースが十分であれば、この画面は表示されず、[ユーザアカウント] 画面でルートアカウントを変更してパスワードを管理できます。

Apex One が Apex Central に登録されていない場合、サポート担当者に Web コンソールへのアクセス方法をお問い合わせください。

Web コンソールの設定

Apex One Web コンソールを設定して、ユーザによる Web コンソールへのアクセス方法と画面更新の頻度を決定します。

手順

1. [管理] > [設定] > [Web コンソール] に移動します。
2. 必要な設定を行います。

セクション	設定
自動表示更新の設定	Apex One サーバが指定された間隔で画面のデータを更新できるようにするには、[Web コンソールの自動更新] を選択します。 • 更新間隔: Web コンソールの画面のデータを更新する頻度 (秒) を選択します。
タイムアウト設定	Apex One サーバが指定された間隔でユーザをログオフできるようにするには、[オフラインユーザを自動的にログオフする] を選択します。 • オフライン間隔: Web コンソールで自動的にオフラインのユーザをログオフするまでの時間 (分) を選択します。

3. [保存] をクリックします。

隔離フォルダ設定

セキュリティエージェントでセキュリティリスクを検出し、検出時の処理が隔離であった場合、感染ファイルを暗号化して、<エージェントインストールフォルダ>¥SUSPECT¥Backup にあるローカルの隔離フォルダに移動します。

ファイルをローカルの隔離ディレクトリに移動した後、セキュリティエージェントはそれを指定された隔離ディレクトリに送信します。[エージェント] > [エージェント管理] > [設定] > {検索の種類} 設定 > [処理] タブで、ディレクトリを指定します。指定された隔離ディレクトリのファイルは、他のファ

イルに感染しないように暗号化されます。詳細については、312 ページの「隔離ディレクトリ」を参照してください。

指定された隔離ディレクトリが、Apex One サーバコンピュータ上にある場合、Web コンソールでサーバの隔離ディレクトリ設定を変更します。サーバでは、隔離ファイルを <サーバインストールフォルダ>¥PCCSRV¥Virus に保存します。

注意

セキュリティエージェントが、何らかの理由で (ネットワーク接続の問題など) 暗号化されたファイルを Apex One サーバに送信できない場合、暗号化されたファイルはセキュリティエージェントの隔離フォルダに残ります。セキュリティエージェントは、Apex One サーバに接続する際にファイルの再送信を試行します。

隔離ディレクトリの設定

手順

1. [管理] > [設定] > [隔離フォルダ設定] に移動します。
2. 隔離フォルダの初期設定の容量、および Apex One で隔離フォルダに保存可能な感染ファイルの最大サイズを、そのまま使用するか変更します。

   初期設定値が画面に表示されます。
3. [隔離フォルダ設定を保存] をクリックします。
4. 隔離フォルダにあるすべての既存ファイルを削除するには、[すべての隔離ファイルを削除] をクリックします。

Server Tuner

Server Tuner を使用すると、次のようなサーバ関連のパフォーマンス問題に対して、パラメータを使用して Apex One サーバのパフォーマンスを最適化することができます。

- ダウンロード

  Apex One サーバにアップデートを要求するセキュリティエージェント数 (アップデートエージェントを含む) が、サーバの使用可能なリソースを超えた場合、サーバはエージェントのアップデート要求をキューに移動して、リソースが使用可能になったときに要求を処理します。エージェントが Apex One サーバからのコンポーネントのアップデートに成功したら、エージェントはサーバにアップデートが完了したことを通知します。Apex One サーバがエージェントからのアップデート通知の受信を待機する最大時間を、分単位で設定します。また、サーバがエージェントに、アップデートの実行と新しい設定の適用の通知を試行する最大回数も設定します。サーバは、エージェントからの通知を受け取らない場合のみ、試行を続けます。

- ネットワークトラフィック

  ネットワークトラフィックの量は、1 日を通して変動します。Apex One サーバおよび他のアップデート元へのネットワークトラフィックフローを制御するには、任意の時点で同時にアップデート可能なセキュリティエージェント数を指定します。

Server Tuner には、次のファイルが必要です。`SvrTune.exe`

Server Tuner の実行

手順

1. Apex One サーバコンピュータで、<サーバインストールフォルダ>`¥PCCSRV¥Admin¥Utility¥SvrTune` に移動します。
2. `SvrTune.exe` をダブルクリックして、Server Tuner を起動します。

   Server Tuner コンソールが開きます。
3. [Download] で、次の設定を変更します。

   - Timeout for client:Apex One サーバがセキュリティエージェントからのアップデートの応答の受信を待機する時間を、分単位で入力します。エージェントがこの時間内に応答しない場合、Apex One サーバは、そのセキュリティエージェントに最新のコンポーネントがイ

ンストールされていないと見なします。通知を受けたセキュリティエージェントがタイムアウトすると、通知を待機している別のエージェントのスロットが使用可能になります。

- Timeout for update agent:Apex One サーバがアップデートエージェントからのアップデートの応答の受信を待機する時間を、分単位で入力します。通知を受けたセキュリティエージェントがタイムアウトすると、通知を待機している別のエージェントのスロットが使用可能になります。
- Retry count:Apex One サーバがセキュリティエージェントに、アップデートの実行または新しい設定の適用の通知を試行する最大回数を設定します。
- Retry interval:Apex One サーバが通知の試行の間に待機する時間を、分単位で指定します。

4. [Network Traffic] で、次の設定を変更します。
   - Normal hours:ネットワークトラフィックの量を通常と判断する時間帯を表すラジオボタンをクリックします。
   - Off-peak hours:ネットワークトラフィックの量を最低と判断する時間帯を表すラジオボタンをクリックします。
   - Peak hours:ネットワークトラフィックの量をピークと判断する時間帯を表すラジオボタンをクリックします。
   - Maximum client connections: 「その他のアップデート元」と Apex One サーバの両方から同時にコンポーネントをアップデートできる、エージェントの最大数を入力します。それぞれの期間に対してエージェントの最大数を入力します。最大接続数に達したとき、セキュリティエージェントがコンポーネントをアップデートできるのは、(アップデートが完了するか、あるいはエージェントの応答が [Timeout for client] または [Timeout for Update Agent] フィールドで指定したタイムアウト値に達したことにより) 現在のセキュリティエージェント接続が閉じられた場合のみです。
5. [OK] をクリックします。Apex One Master Service を再起動するよう求めるメッセージが表示されます。

注意

再起動するのはサービスのみであり、コンピュータではありません。

6. 次の再起動オプションから選択します。
   - [Yes] をクリックすると、Server Tuner 設定が保存され、サービスが再起動されます。再起動するとただちに設定が有効になります。
   - [No] をクリックすると、Server Tuner 設定は保存されますが、サービスは再起動されません。設定を有効にするには、Apex One Master Service または Apex One サーバコンピュータを再起動してください。

スマートフィードバック

スマートフィードバックを有効にすると、コンピュータで検出された脅威に関する情報 (アクセスされた Web アドレス、ファイルに関する情報等) がトレンドマイクロに送信され、新たな脅威の迅速な識別や対処に役立てられます。お客さまから収集された情報の取り扱いについての詳細はこちら、プライバシーと個人データの収集に関する規定についてはこちらにてご確認いただけます。

スマートフィードバックプログラムへの参加

手順

1. [管理] > [Smart Protection] > [スマートフィードバック] に移動します。
2. [Trend Micro スマートフィードバックを有効にする] をクリックします。
3. トレンドマイクロが統計上の参考とするため、[業種] を選択します。
4. セキュリティエージェント上のファイルにおける潜在的なセキュリティ上の脅威に関する情報を送信するには、[不審プログラムファイルのフィードバックを有効にする] チェックボックスをオンにします。

注意

お客さまから収集された情報の取り扱いについての詳細は http://www.go-tm.jp/legal-spn よりご確認いただけます。

5. フィードバックの送信条件として、特定の期間内に検出される脅威の数を指定します。
6. ネットワークの中断を避けるために、フィードバック送信時に Apex One が使用できる最大帯域幅を指定します。
7. [保存] をクリックします。

第 15 章

セキュリティエージェントの管理

この章では、セキュリティエージェントの管理と設定について説明します。

この章は次のトピックで構成されます。

エンドポイント(コンピュータ)の位置

Apex One は、セキュリティエージェントが内部ネットワークと外部ネットワークのどちらにあるかを判定する位置認識機能を備えています。位置認識機能は、次の Apex One の機能やサービスで利用されています。

表 15-1. 位置認識機能を利用する機能とサービス

機能/サービス	説明
ファイルレピュテーションサービス	スマートスキャンエージェントでは、セキュリティエージェントが検索クエリを送信する Smart Protection ソースがセキュリティエージェントの位置によって判定されます。 検索クエリの送信先は、外部セキュリティエージェントの場合は Trend Micro Smart Protection Network となり、内部セキュリティエージェントの場合は Trend Micro Smart Protection ソースリストに定義されているソースになります。 詳細については、106 ページの「Trend Micro Smart Protection ソース」を参照してください。
Web レピュテーション 情報漏えい対策 デバイスコントロール	セキュリティエージェントが内部と外部のどちらのポリシー設定を適用するかがセキュリティエージェントの位置によって判定されます。通常、管理者は、外部セキュリティエージェントに対してより厳格なポリシーを設定します。 詳細については、次のページを参照してください。 • 517 ページの「Web レピュテーションポリシー」 • 453 ページの「情報漏えい対策のポリシー」 • 432 ページの「デバイスコントロール」

位置の基準

その位置を、セキュリティエージェントエンドポイントのゲートウェイ IP アドレスに基づいて判断するか、Apex One サーバや参照サーバとのセキュリティエージェントの接続状態に基づいて判断するかを指定します。

- エージェントの接続状態: セキュリティエージェントがインターネット上の Apex One サーバまたは参照サーバに接続できる場合、そのエンドポイントの位置は「内部」と見なされます。さらに、企業のネットワーク

の外部にあるエンドポイントが Apex One サーバまたは参照サーバと接続を確立できる場合も、そのエンドポイントの位置は「内部」と見なされます。これら以外の場合、エンドポイントの位置は「外部」と見なされます。

- ゲートウェイ IP アドレスおよび MAC アドレス: セキュリティエージェントエンドポイントのゲートウェイ IP アドレスが、[エンドポイントの位置] 画面で指定したゲートウェイ IP アドレスのいずれかと一致する場合、そのエンドポイントの位置は「内部」と見なされます。一致しない場合は、エンドポイントの位置は「外部」と見なされます。

位置設定

手順

1. [エージェント] > [エンドポイントの位置] に移動します。
2. 位置の基準を、[エージェントの接続状態] にするか、または [ゲートウェイ IP アドレス] および [MAC アドレス] にするか選択します。
3. [エージェントの接続状態] を選択した場合、参照サーバを使用するかどうかを決定します。

   詳細については、610 ページの「参照サーバ」を参照してください。

   a. 参照サーバを指定しなかった場合、次のイベントが発生したときに、セキュリティエージェントは Apex One サーバとの接続状態をチェックします。

      - セキュリティエージェントがスタンドアロンモードから通常の (オンライン/オフライン) モードに切り替えたとき
      - セキュリティエージェントがある検索方法から別の検索方法に切り替えたとき

        詳細については、279 ページの「検索方法の種類」を参照してください。

      - セキュリティエージェントがエンドポイントの IP アドレスの変更を検出したとき

- セキュリティエージェントが再起動したとき
- サーバが接続状態の確認を開始したとき

  詳細については、664 ページの「セキュリティエージェントのアイコン」を参照してください。
- グローバル設定を適用する際に Web レピュテーションの位置の基準が変更されたとき
- 大規模感染予防ポリシーが実行されなくなり、大規模感染前の設定が復元されたとき

b. 参照サーバを指定した場合、セキュリティエージェントではまず Apex One サーバとの接続状態がチェックされ、Apex One サーバとの接続が成功していない場合は参照サーバとの接続状態がチェックされます。セキュリティエージェントによる接続状態のチェックは 1 時間ごとに行われ、さらに前述のいずれかのイベントが発生したときも行われます。

4. [ゲートウェイ IP アドレス] および [MAC アドレス] を選択した場合、次の処理を実行します。

   a. 表示されたテキストボックスに、ゲートウェイの IPv4/IPv6 アドレスを入力します。

   b. MAC アドレスを入力します。

   c. [追加] をクリックします。

      MAC アドレスを入力しない場合、Apex One には指定された IP アドレスに属するすべての MAC アドレスが指定されます。

   d. 追加するすべてのゲートウェイ IP アドレスに対して手順 a～c を繰り返します。

   e. ゲートウェイ設定インポートツールを使用して、ゲートウェイ設定のリストをインポートします。

      詳細については、643 ページの「ゲートウェイ設定インポートツール」を参照してください。

5. [保存] をクリックします。

ゲートウェイ設定インポートツール

Apex One は、エンドポイントの位置をチェックして、使用する Web レピュテーションポリシーと接続先の Trend Micro Smart Protection ソースを決定します。Apex One で位置を識別する方法の 1 つは、エンドポイントのゲートウェイ IP アドレスと MAC アドレスをチェックすることです。

エンドポイントの位置 画面でゲートウェイの設定を行うか、ゲートウェイ設定インポートツールを使用してゲートウェイ設定のリストを エンドポイントの位置 画面にインポートします。

ゲートウェイ設定インポートツールの使用

手順

1. ゲートウェイ設定のリストが格納されたテキストファイル (`.txt`) を用意します。各行には IPv4 または IPv6 アドレスを入力し、必要に応じて MAC アドレスを入力します。

   IP アドレスと MAC アドレスは、カンマで区切ります。エントリの最大数は 4096 です。

   次に例を示します。

   ```
   10.1.111.222,00:17:31:06:e6:e7

   2001:0db7:85a3:0000:0000:8a2e:0370:7334

   10.1.111.224,00:17:31:06:e6:e7
   ```

2. サーバコンピュータで、<サーバインストールフォルダ>`¥PCCSRV¥Admin¥Utility¥GatewaySettingsImporter` に移動します。

3. `GSImporter.exe` を右クリックして、[管理者として実行] を選択します。

注意

ターミナルサービスからゲートウェイ設定インポートツールを実行することはできません。

4. [ゲートウェイ設定インポートツール] 画面で、手順 1 で作成したファイルを指定して [インポート] をクリックします。
5. [OK] をクリックします。

   エンドポイントの位置 画面にゲートウェイの設定が表示され、Apex One サーバはセキュリティエージェントに設定を配信します。
6. すべてのエントリを削除するには、[すべてクリア] をクリックします。

   特定のエントリのみを削除する必要がある場合、エンドポイントの位置の画面からそのエントリを削除します。
7. 設定をファイルにエクスポートするには、[すべてエクスポート] をクリックし、ファイルの名前と種類を指定します。

セキュリティエージェントプログラムの管理

ここでは、セキュリティエージェントプログラムの管理および保護方法について説明します。

- 645 ページの「セキュリティエージェントサービス」
- 652 ページの「セキュリティエージェントサービスの再起動」
- 653 ページの「セキュリティエージェントコンソールアクセス制限」
- 655 ページの「セキュリティエージェントのアンロードとロック解除」
- 656 ページの「セキュリティエージェントのスタンドアロンモード権限」
- 659 ページの「セキュリティエージェント言語設定」
- 660 ページの「エージェント移動ツール」
- 663 ページの「オフラインのセキュリティエージェント」

セキュリティエージェントサービス

セキュリティエージェントは、次の表に示すサービスを実行します。Microsoft 管理コンソールから、これらのサービスの状態を確認できます。

表 15-2. 初期設定のプロセス

プロセス名	説明	位置
TmListen.exe	Apex One サーバからコマンドと通知を受信して、セキュリティエージェントからサーバへの通信を制御します。	<エージェントのインストールフォルダ>\tmlisten.exe
NTRtScan.exe	セキュリティエージェントでリアルタイム検索、予約検索、および手動検索を実行します。	<エージェントのインストールフォルダ>\ntrtscan.exe
TmPfw.exe	パケットレベルファイアウォールおよびネットワークウイルス検索機能を提供します。	<エージェントのインストールフォルダ>\TmPfw.exe
TMBMSRV.exe	外部ストレージデバイスへのアクセスを規制し、レジストリキーおよびプロセスへの不正な変更を回避します。 注意 このオプションを有効にすると、エンドポイントへの他社製品のインストールがセキュリティエージェントによって阻止されることがあります。この問題が発生した場合は、このオプションを一時的に無効にして他社製品をインストールし、その後再びこのオプションを有効化してください。	<%Program Files (x86) フォルダ%>\Trend Micro\BM\TMBMSRV.exe
TmCCSF.exe	ブラウザ脆弱性対策およびメモリ検索を実行します。	<エージェントのインストールフォルダ>\CCSF\TmCCSF.exe

プロセス名	説明	位置
TmWSCSvc.exe	Apex One セキュリティエージェントのセキュリティステータスを Security Center に報告します。	<エージェントのインストールフォルダ>\TmWSCSvc.exe

表 15-3. 拡張機能のプロセス

プロセス名	説明	位置
DSAgent.exe	機密データの転送を監視し、デバイスへのアクセスを管理します。	<%Windows ディレクトリ%>\system32\dgagent\DSAGENT.exe
ATASAgent.exe	高度な Managed Detection and Response タスクと通信	<%Program Files (x86) フォルダ%>\Trend Micro\iService\iATAS\ATASAgent.exe
TMiACAgentSvc.exe	Trend Micro Application Control Service (Agent)	<%Program Files (x86) フォルダ%>\Trend Micro\iService\iAC\ac_bin\TMiACAgentSvc.exe
ESEServiceShell.exe	Trend Micro Endpoint Sensor Engine Wrapper	<%Program Files (x86) フォルダ%>\Trend Micro\iService\iES\ESE\ESEServiceShell.exe

プロセス名	説明	位置
ESClient.exe	Trend Micro Endpoint Sensor Service (Agent)	C:\Program Files (x86)\Trend Micro\iService \iES\ESE \ESClient.exe
iVPAgent.exe	Trend Micro Vulnerability Protection Service (Agent)	<%Program Files (x86) フォルダ%>\Trend Micro\iService \iVP \iVPAgent.exe

次の各サービスは強力な保護機能を提供しますが、これらのサービスの監視メカニズムがシステムリソースの負荷となる場合があります。特に、システム負荷の高いアプリケーションを実行するサーバでは、システムリソースに重い負荷がかかることがあります。

- Trend Micro Unauthorized Change Prevention Service (TMBMSRV.exe)
- Apex One NT Firewall (TmPfw.exe)
- Apex One Data Protection Service (dsagent.exe)

そのため、Windows Server プラットフォームではこれらのサービスが初期設定で無効になっています。これらのサービスを有効にする場合は、次の点を考慮してください。

- システムのパフォーマンスを継続的に監視し、パフォーマンスの低下を認識した時点で必要な措置を取るようにします。
- 「TMBMSRV.exe」については、システム負荷の高いアプリケーションを挙動監視ポリシーから除外した上でこのサービスを有効にしてください。システム負荷の高いアプリケーションは、パフォーマンス調整ツールを使って特定できます。

  詳細については、652 ページの「Trend Micro パフォーマンス調整ツールの使用」を参照してください。

デスクトッププラットフォームに対しては、パフォーマンスの大幅な低下が見られた場合にのみ、このサービスを無効にします。

他社製アプリケーションにおけるセキュリティエージェントサービスとプロセスの除外

次の表は、他社製アプリケーションからの除外が必要となる可能性のあるセキュリティエージェントのプロセスの名前とファイルのフルパスを示しています。

表 15-4. 初期設定のプロセス

プロセス名	説明	位置
TmListen.exe	Apex One サーバからコマンドと通知を受信して、セキュリティエージェントからサーバへの通信を制御します。	<エージェントのインストールフォルダ>\tmlisten.exe
NTRtScan.exe	セキュリティエージェントでリアルタイム検索、予約検索、および手動検索を実行します。	<エージェントのインストールフォルダ>\ntrtscan.exe
TmPfw.exe	パケットレベルファイアウォールおよびネットワークウイルス検索機能を提供します。	<エージェントのインストールフォルダ>\TmPfw.exe
TMBMSRV.exe	外部ストレージデバイスへのアクセスを規制し、レジストリキーおよびプロセスへの不正な変更を回避します。 **注意** このオプションを有効にすると、エンドポイントへの他社製品のインストールがセキュリティエージェントによって阻止されることがあります。この問題が発生した場合は、このオプションを一時的に無効にして他社製品をインストールし、その後再びこのオプションを有効化してください。	<%Program Files (x86) フォルダ%>\Trend Micro\BM\TMBMSRV.exe
TmCCSF.exe	ブラウザ脆弱性対策およびメモリ検索を実行します。	<エージェントのインストールフォルダ>\CCSF\TmCCSF.exe

プロセス名	説明	位置
TmWSCSvc.exe	Apex One セキュリティエージェントのセキュリティステータスを Security Center に報告します。	<エージェントのインストールフォルダ>\TmWSCSvc.exe

表 15-5. 拡張機能のプロセス

プロセス名	説明	位置
DSAgent.exe	機密データの転送を監視し、デバイスへのアクセスを管理します。	<%Windows ディレクトリ%>\system32\dgagent\DSAGENT.exe
ATASAgent.exe	高度な Managed Detection and Response タスクと通信	<%Program Files (x86) フォルダ%>\Trend Micro\iService\iATAS\ATASAgent.exe
TMiACAgentSvc.exe	Trend Micro Application Control Service (Agent)	<%Program Files (x86) フォルダ%>\Trend Micro\iService\iAC\ac_bin\TMiACAgentSvc.exe
ESEServiceShell.exe	Trend Micro Endpoint Sensor Engine Wrapper	<%Program Files (x86) フォルダ%>\Trend Micro\iService\iES\ESE\ESEServiceShell.exe

プロセス名	説明	位置
ESClient.exe	Trend Micro Endpoint Sensor Service (Agent)	C:\Program Files (x86)\Trend Micro\iService \iES\ESE \ESClient.exe
iVPAgent.exe	Trend Micro Vulnerability Protection Service (Agent)	<%Program Files (x86) フォルダ%>\Trend Micro\iService \iVP \iVPAgent.exe

表 15-6. 追加の保護されたプロセス

プロセス名	位置
ShowMsg.exe	<%Windows ディレクトリ%>\System32\ShowMsg.exe
TmSSClient.exe	<エージェントのインストールフォルダ r>\TmSSClient.exe
LogServer.exe	<エージェントのインストールフォルダ>\Temp\LogServer \LogServer.exe
TmsaInstance64.exe	<エージェントのインストールフォルダ>\CCSF\module\BES \TmsaInstance64.exe
CNTAoSMgr.exe	<エージェントのインストールフォルダ>\CNTAoSMgr.exe
ESEFrameworkHost.exe	<%Program Files (x86) フォルダ%>\Trend Micro\iService\iES\ESE \ESEFrameworkHost.exe

セキュリティエージェントの追加サービス設定

重要

Windows Server プラットフォームで追加のサービスを有効にすると、サーバのパフォーマンスが低下することがあります。Windows Server プラットフォームでサービスを有効にした後、しばらくはサーバを監視して、パフォーマンスへの影響がないことを確認することをお勧めします。

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [追加サービス設定] をクリックします。
4. 次のセクションの [Windows デスクトップ] または [Windows Server プラットフォーム] で必要なサービスを選択して有効にします。
   - 不正変更防止サービス

     Windows Server プラットフォームの場合、有効にする保護レベルを選択します。
     - フルモード: すべてのサービスを有効にし、すべての機能へのフルアクセスを提供します。
     - パフォーマンスモード: 次に示す機能だけを有効にして、フルモードで使用可能なその他の設定をすべて無視する軽量バージョンのサービスを実現します。
       - [挙動監視] > [不正プログラム挙動ブロックを有効にする] > [不正な暗号化や変更からの文書の保護]

       重要

       パフォーマンスモードでは、設定が自動的に有効になることはありません。特定の機能を有効にすると、不正変更防止サービスにより、サポートされる機能だけが有効になり、サポートされない設定はすべて無視されます。
   - ファイアウォールサービス

     重要

     サービスを有効または無効にすると、エンドポイントが一時的にネットワークから切断されます。切断の影響を最小にするため、就業時間帯は設定の変更を避けてください。

- 不審接続監視サービス
- 情報漏えい対策オプションサービス

重要

サービスを有効または無効にすると、エンドポイントが一時的にネットワークから切断されます。切断の影響を最小にするため、就業時間帯は設定の変更を避けてください。

- 高度な保護サービス

5. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。
   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
   - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

Trend Micro パフォーマンス調整ツールの使用

Trend Micro パフォーマンス調整ツールについては、次を参照してください。

https://success.trendmicro.com/jp/solution/1310435

セキュリティエージェントサービスの再起動

Apex One は、予期せず応答を停止したが、通常のシステムプロセスでは停止しなかったセキュリティエージェントサービスを再起動します。エージェントサービスの詳細については、645 ページの「セキュリティエージェントサービス」を参照してください。

セキュリティエージェントサービスの再起動を有効にするには、必要な設定を行います。

サービスの再起動の設定

手順

1. [エージェント] > [グローバルエージェント設定]に移動します。
2. [システム] タブをクリックします。
3. [サービスの再起動] セクションに移動します。
4. [セキュリティエージェントサービスが予期せず停止した場合はサービスを自動的に再起動する] を選択します。
5. 次の設定を行います。
   - __分後にサービスを再起動:Apex One がサービスを再起動するまでの時間を分単位で指定します。
   - サービスの再起動に失敗した後、__回まで再試行する: サービスを再起動するための最大再試行回数を指定します。再試行を最大回数実行しても停止したままであれば、サービスを手動で再起動します。
   - __時間後に再起動エラー回数をリセットする: 再試行を最大回数実行してもサービスが停止したままである場合、Apex One は指定された時間 (時単位) 待機して、失敗のカウントをリセットします。指定された時間が経過してもサービスが停止したままであれば、Apex One はサービスを再起動します。

セキュリティエージェントコンソールアクセス制限

この設定を使用すると、タスクトレイまたは Windows の [スタート] メニューからセキュリティエージェントコンソールにアクセスできなくなります。ユーザがセキュリティエージェントコンソールにアクセスするためには、<エージェントインストールフォルダ>から `PccNTMon.exe` をダブルクリックする必要があります。この設定を行った後、セキュリティエージェントを再起動して設定を有効にします。

この設定によってセキュリティエージェントが無効になることはありません。セキュリティエージェントは引き続きバックグラウンドで動作し、セキュリティリスクからコンピュータを保護します。

セキュリティエージェントコンソールへのアクセスの制限

手順

1. [エージェント] > [エージェント管理]に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [その他の設定] タブをクリックし、[セキュリティエージェントアクセス制限] セクションに移動します。
5. [システムトレイあるいは Windows スタートメニューからセキュリティエージェントコンソールへのアクセスを許可しない] を選択します。
6. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。
   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
   - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

セキュリティエージェントのアンロードとロック解除

セキュリティエージェントのアンロードとロック解除権限を持つユーザは、パスワードの有無に関係なく、セキュリティエージェントを一時的に停止することも、高度な Web コンソール機能にアクセスすることもできます。

エージェントのアンロードとロック解除権限の付与

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [権限] タブの [アンロードとロック解除] セクションに移動します。
5. パスワードの要件を設定します。
   - パスワードを要求しない
   - パスワードを要求する: 必要なパスワードと確認用のパスワードを入力します。

     注意

     パスワードは以下の複雑さの要件を満たしている必要があります。
     - 8～32 文字の長さ
     - 大文字 (A～Z)、小文字 (a～z)、数字 (0～9)、特殊文字をそれぞれ 1 文字以上含む
     - 印刷できない ASCII 文字を含まない
6. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。

- すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
- 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

セキュリティエージェントのスタンドアロンモード権限

エージェント/サーバイベントによってユーザのタスクが妨害される場合は、そのユーザにセキュリティエージェントのスタンドアロンモード権限を付与します。たとえば、頻繁にプレゼンテーションを行うユーザの場合、プレゼンテーションの開始前にスタンドアロンモードを有効にすることによって、Apex One サーバからセキュリティエージェント設定が配信されセキュリティエージェントで検索が開始されるのを阻止できます。

スタンドアロンモード時のセキュリティエージェントの動作:

- サーバとエージェント間の接続が機能していても、セキュリティエージェントは Apex One サーバにログを送信しません。
- サーバとエージェント間の接続が機能していても、Apex One サーバは、タスクの開始も、エージェントへのセキュリティエージェント設定の配信も行いません。
- セキュリティエージェントは、いずれかのアップデート元への接続が可能なら、コンポーネントをアップデートします。アップデート元には、Apex One サーバ、アップデートエージェント、ユーザ指定のアップデート元などがあります。

  次のイベントによって、スタンドアロンエージェントでアップデートが開始されます。

  - ユーザによる手動アップデートの実行。
  - エージェントの自動アップデートの実行。スタンドアロンエージェントでは、エージェントの自動アップデートを無効に設定できます。

詳細については、658 ページの「スタンドアロンエージェントでのエージェントの自動アップデートの無効化」を参照してください。

- 予約アップデートの実行。予約アップデートは、必要な権限を持つエージェントのみ実行できます。この権限はいつでも取り消すことができます。

  詳細については、658 ページの「Apex One スタンドアロンエージェントでの予約アップデート権限の取り消し」を参照してください。

エージェントのスタンドアロンモード権限の付与

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [権限] タブの [スタンドアロンモード] セクションに移動します。
5. [スタンドアロンモードの有効化] を選択します。
6. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。

   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
   - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

スタンドアロンエージェントでのエージェントの自動アップデートの無効化

手順

1. [アップデート] > [エージェント] > [自動アップデート]に移動します。
2. [イベント起動配信] セクションに移動します。
3. [スタンドアロンモードおよびオフラインモードのエージェントを含む] を無効にします。

> **注意**
>
> このオプションは、[Apex One サーバが新しいコンポーネントをダウンロード後、ただちにエージェントのコンポーネントのアップデートを開始する] を無効にすると、自動的に無効になります。

Apex One スタンドアロンエージェントでの予約アップデート権限の取り消し

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックするか、特定のドメインまたはエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [権限] タブの [コンポーネントのアップデート] セクションに移動します。
5. [予約アップデートの有効化/無効化] オプションをオフにします。
6. [保存]をクリックします。

セキュリティエージェント言語設定

すべてのセキュリティエージェントを Apex One サーバの言語設定または ローカルのログオンユーザの言語設定のどちらかを使用して表示するように 設定することができます。セキュリティエージェントプログラムをインス トールまたはバージョンアップした後、[グローバル設定] 画面で設定した言語 設定が適用されます。

初期設定では、ログオンユーザの言語設定がセキュリティエージェントでサ ポートされていない場合は、Apex One サーバの言語 (日本語) が使用されま す。

セキュリティエージェントの言語設定

手順

1. [エージェント] > [グローバルエージェント設定]に移動します。
2. [エージェント制御] タブをクリックします。
3. [エージェント言語設定] セクションに移動します。
4. セキュリティエージェントでの言語設定の適用オプションを指定しま す。
   - エンドポイントのローカルの言語設定: セキュリティエージェント は、ログオンしているユーザの言語設定を使用して表示されます。

     注意

     ログオンしているユーザの言語設定がセキュリティエージェントでサ ポートされていない場合は、Apex One サーバの言語が適用されます。 Apex One サーバの言語がサポートされていない場合は、英語で表示さ れます。
   - Apex One サーバの言語: セキュリティエージェントは、Apex One サーバの言語を使用して表示されます。

注意

Apex One サーバの言語がサポートされていない場合は、英語で表示されます。

5. [保存]をクリックします。

エージェント移動ツール

ネットワーク上に複数の Apex One サーバがある場合、Apex One サーバ間でセキュリティエージェントを移動するには、エージェント移動ツールを使用します。これは特に、新しい Apex One サーバをネットワークに追加した後、既存のセキュリティエージェントを新しいサーバに移動する場合に役立ちます。

注意

移動元と移動先のサーバの言語バージョンが同じである必要があります。エージェント移動ツールを使用して、従来のバージョンが稼働しているセキュリティエージェントを現在のバージョンのサーバに移動すると、セキュリティエージェントは自動的にバージョンアップされます。

このツールを使用する前に、使用するアカウントが管理者権限を持っていることを確認してください。

エージェント移動ツールの実行

手順

1. Apex One サーバで<サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility¥IpXfer に移動します。
2. 「IpXfer.exe」をセキュリティエージェントエンドポイントにコピーします。セキュリティエージェントエンドポイントが x64 タイプのプラットフォームで稼働している場合は、代わりに「IpXfer_x64.exe」をコピーします。
3. セキュリティエージェントエンドポイント上でコマンドプロンプトを開いて、実行可能ファイルのコピー先フォルダに移動します。

4. 次の構文を使用して、エージェント移動ツールを実行します。

   <実行可能ファイル名> -s <サーバ名> -p <サーバ待機ポート> -c <エージェント待機ポート> -d <ドメインまたはドメイン階層> -e <証明書の場所およびファイル名> -pwd <エージェントのアンロードおよびアンロックの権限パスワード>

   表 15-7. エージェント移動ツールのパラメータ

パラメータ	説明
<実行可能ファイル名>	IpXfer.exe または IpXfer_x64.exe
-s <サーバ名>	セキュリティエージェントの移動先となる Apex One サーバの名前。
-p <サーバ待機ポート>	移動先の Apex One サーバの待機ポート(または信頼されたポート) (ローカルサーバのみ) Web コンソールに待機ポートを表示するには、メインメニューで [管理] > [設定] > [エージェント接続] をクリックします。
-sp <サーバの HTTPS 待機ポート>	移動先の Apex One サーバの HTTPS 通信用待機ポート (または信頼されたポート)。
-c <エージェント待機ポート>	セキュリティエージェントエンドポイントがサーバとの通信に使用するポート番号。
-d <ドメインまたはドメイン階層>	エージェントをグループメンバーとして追加するエージェントツリーのドメインまたはサブドメイン。 ドメイン階層にはサブドメインを指定する必要があります。

パラメータ	説明
-e <証明書の場所およびファイル名>	移動処理時にセキュリティエージェントの新しい認証証明書をインポートします。 このパラメータを使用しない場合、新しい管理サーバから現在の認証証明書が自動的に取得されます。 **注意** 初期設定では、証明書は Apex One サーバ上の次の場所にあります。 <サーバインストールフォルダ>¥PCCSRV¥Pccnt¥Common¥OfcNTCer.dat Apex One 以外のソースから証明書を使用する場合は、DER (Distinguished Encoding Rules) 形式の証明書であることを確認してください。
-pwd <エージェントのアンロードおよびアンロックの権限パスワード>	[権限とその他の設定] で設定したアンロード/アンロック権限パスワード。 **注意** アンロード/アンロックパスワードが必要な場合にパスワードを指定せずにエージェント移動ツールを実行すると、エージェントの移動前に指定するように求められます。
-dbg	接続のデバッグログを有効にします。

例:

- HTTP 通信を使用する Apex One サーバの場合:

  ```
  ipXfer.exe -s Server01 -p 8080 -c 21112 -d Workgroup -pwd unlock
  ```

  ```
  ipXfer_x64.exe -s Server02 -p 8080 -c 21112 -d Workgroup\Group01 -pwd unlock
  ```

- HTTPS 通信を使用する Apex One サーバの場合:

```
ipXfer.exe -s Server01 -sp 443 -p 8080 -c 21112 -d
Workgroup -pwd unlock -dbg 1
```

5. 別のサーバに対するセキュリティエージェントの現在のレポートを確認するには、次の処理を実行します。

   a. セキュリティエージェントエンドポイントで、タスクトレイにあるセキュリティエージェントプログラムのアイコンを右クリックします。

   b. [コンポーネントのバージョン] を選択します。

   c. [サーバ名/ポート] フィールドで、セキュリティエージェントのレポート先となる Apex One サーバを確認します。

   注意

   新しい Apex One サーバが管理するエージェントツリーにそのセキュリティエージェントが表示されない場合、新しいサーバのマスターサービス (ofservice.exe) を再起動します。

オフラインのセキュリティエージェント

セキュリティエージェントのアンインストールプログラムを使用して、エンドポイントからセキュリティエージェントプログラムを削除した場合、自動的にサーバに通知されます。この通知を受け取ったサーバは、そのエージェントが存在しないことがわかるように、エージェントツリーからそのセキュリティエージェントのアイコンを削除します。

ただし、エンドポイントのハードディスクを再フォーマットしたり、セキュリティエージェントファイルを手動で削除するなどの別の方法を使用してセキュリティエージェントを削除した場合、Apex One では削除されたことを認識できず、セキュリティエージェントはオフラインとして表示されます。ユーザがセキュリティエージェントをアンロードしたり長期間無効にした場合も、セキュリティエージェントはオフラインとして表示されます。

エージェントツリーにオンラインのエージェントのみを表示させるには、エージェントツリーからオフラインエージェントを自動的に削除するように、Apex One を設定します。

オフラインエージェントの自動削除

手順

1. [管理] > [設定] > [オフラインエージェント]に移動します。
2. [オフラインエージェントの自動削除機能を有効にする] を選択します。
3. Apex One がセキュリティエージェントをオフラインと見なすまでの経過日数を選択します。
4. [保存]をクリックします。

エージェントとサーバ間の接続

セキュリティエージェントでは、コンポーネントのアップデート、通知の受信、および設定変更の適用を適切なタイミングで行えるよう、親サーバとの接続を常に維持する必要があります。ここでは、セキュリティエージェントの接続状態の確認方法と、接続の問題の解決方法について説明します。

- 664 ページの「セキュリティエージェントのアイコン」
- 680 ページの「エージェントとサーバ間の接続の確認」
- 681 ページの「接続状態の確認ログ」
- 682 ページの「到達不能エージェント」

セキュリティエージェントのアイコン

タスクトレイのセキュリティエージェントのアイコンは、セキュリティエージェントの現在の状態や、ユーザへの特定の処理の実行要求など、視覚的なヒントを示します。アイコンは常に、次の視覚的なヒントを組み合わせて表示されます。

表 15-8. セキュリティエージェントのアイコンが示すセキュリティエージェントの状態

エージェントステータス	説明	視覚的なヒント
エージェントと Apex One サーバとの接続	オンラインエージェントは Apex One サーバに接続されています。サーバでは、これらのエージェントに対してタスクを起動したり、設定を配信したりできます。	アイコンには心拍に似たシンボルが表示されます。  背景色には、リアルタイム検索サービスの状態に応じて青または赤の陰影が付けられます。
	オフラインエージェントは Apex One サーバと接続されていません。サーバは、この状態のエージェントを管理できません。	アイコンには心拍の消失に似たシンボルが表示されます。  背景色には、リアルタイム検索サービスの状態に応じて青または赤の陰影が付けられます。 エージェントがネットワークに接続されていても、オフラインになっている可能性があります。この問題の詳細については、677 ページの「セキュリティエージェントアイコンが示す問題の解決方法」を参照してください。
	スタンドアロンエージェントは、Apex One サーバと通信できる場合と、できない場合があります。	アイコンにはデスクトップと信号のシンボルが表示されます。  背景色には、リアルタイム検索サービスの状態に応じて青または赤の陰影が付けられます。 スタンドアロンモードのエージェントの詳細については、656 ページの「セキュリティエージェントのスタンドアロンモード権限」を参照してください。

エージェントステータス	説明	視覚的なヒント
Trend Micro Smart Protection ソースの使用可否	Trend Micro Smart Protection ソースには、Smart Protection Server と Trend Micro Smart Protection Network があります。 従来型のスキャンエージェントは、Web レピュテーションクエリの目的で Trend Micro Smart Protection ソースに接続します。 スマートスキャンエージェントは、検索クエリと Web レピュテーションクエリの目的で Trend Micro Smart Protection ソースに接続します。	Trend Micro Smart Protection ソースが使用可能な場合は、アイコンにチェックマークが表示されます。 
		使用可能な Trend Micro Smart Protection ソースがないときに、エージェントがソースとの接続を確立しようとしている場合は、アイコンに進行状況のバーが表示されます。  この問題の詳細については、677 ページの「セキュリティエージェントアイコンが示す問題の解決方法」を参照してください。
		従来型スキャンエージェントでは、そのエージェントで Web レピュテーションが無効に設定されている場合、チェックマークも進行状況のバーも表示されません。

エージェントステータス	説明	視覚的なヒント
リアルタイム検索サービスの状態	Apex One は、リアルタイム検索サービスをリアルタイム検索だけでなく、手動検索や予約検索にも使用します。 このサービスが機能していないと、エージェントがセキュリティリスクにさらされます。	リアルタイム検索サービスが機能している場合は、青で塗りつぶしたアイコンが表示されます。エージェントの検索方法によって青色の濃さが異なります。 • 従来型スキャンの場合:  • スマートスキャンの場合: 
		リアルタイム検索サービスが無効になっているか機能していない場合は、アイコン全体が赤い陰影で表示されます。 エージェントの検索方法によって赤色の濃さが異なります。 • 従来型スキャンの場合:  • スマートスキャンの場合:  この問題の詳細については、677 ページの「セキュリティエージェントアイコンが示す問題の解決方法」を参照してください。

エージェントステータス	説明	視覚的なヒント
リアルタイム検索の状態	リアルタイム検索は積極的な保護機能を提供し、ファイルの作成、変更、または取得時に、そのファイルにセキュリティリスクが存在するかどうかを検索します。	リアルタイム検索が有効になっているかどうかの視覚的なヒントはありません。
		リアルタイム検索が無効になっている場合は、アイコン全体が赤い円で囲まれ、中に赤い斜線が表示されます。  この問題の詳細については、677 ページの「セキュリティエージェントアイコンが示す問題の解決方法」を参照してください。
パターンファイルのアップデートの状態	最新の脅威からエージェントを保護するには、エージェントのパターンファイルを定期的にアップデートする必要があります。	パターンファイルが最新か、または少し古くなっているかを示す視覚的なヒントはありません。
		パターンファイルが著しく古い場合は、アイコンに感嘆符が表示されます。これはパターンファイルがしばらくアップデートされていないことを意味します。  エージェントのアップデート方法の詳細については、231 ページの「セキュリティエージェントのアップデート」を参照してください。
Apex One サーバ体験版のステータス	オンラインエージェントは、体験版期間が終了した Apex One サーバに接続されています。	Apex One サーバの体験版期間が終了している場合、次のアイコンが表示されます。 

スマートスキャンのアイコン

セキュリティエージェントでスマートスキャンを使用している場合は、次のいずれかのアイコンが表示されます。

表 15-9. スマートスキャンのアイコン

アイコン	Apex One サーバとの接続	Trend Micro Smart Protection ソースの使用可否	リアルタイム検索サービス	リアルタイム検索
	オンライン	使用可能	機能しています	有効
	オンライン	使用可能	機能しています	無効
	オンライン	使用可能	無効または機能していません	無効または機能していません
	オンライン	使用不可、ソースに再度接続しています	機能しています	有効
	オンライン	使用不可、ソースに再度接続しています	機能しています	無効
	オンライン	使用不可、ソースに再度接続しています	無効または機能していません	無効または機能していません
	オフライン	使用可能	機能しています	有効
	オフライン	使用可能	機能しています	無効
	オフライン	使用可能	無効または機能していません	無効または機能していません
	オフライン	使用不可、ソースに再度接続しています	機能しています	有効
	オフライン	使用不可、ソースに再度接続しています	機能しています	無効

アイコン	APEX ONE サーバとの接続	TREND MICRO SMART PROTECTION ソースの使用可否	リアルタイム検索サービス	リアルタイム検索
	オフライン	使用不可、ソースに再度接続しています	無効または機能していません	無効または機能していません
	スタンドアロン	使用可能	機能しています	有効
	スタンドアロン	使用可能	機能しています	無効
	スタンドアロン	使用可能	無効または機能していません	無効または機能していません
	スタンドアロン	使用不可、ソースに再度接続しています	機能しています	有効
	スタンドアロン	使用不可、ソースに再度接続しています	機能しています	無効
	スタンドアロン	使用不可、ソースに再度接続しています	無効または機能していません	無効または機能していません

従来型スキャンのアイコン

セキュリティエージェントで従来型スキャンを使用している場合は、次のいずれかのアイコンが表示されます。

表 15-10. 従来型スキャンのアイコン

アイコン	Apex One サーバとの接続	Trend Micro Smart Protection ソースで提供される Web レピュテーションサービス	リアルタイム検索サービス	リアルタイム検索	ウイルスパターンファイル
	オンライン	使用可能	機能しています	有効	最新またはやや古い
	オンライン	使用不可、ソースに再度接続しています	機能しています	有効	最新またはやや古い
	オンライン	使用可能	機能しています	有効	著しく古い
	オンライン	使用不可、ソースに再度接続しています	機能しています	有効	著しく古い
	オンライン	使用可能	機能しています	無効	最新またはやや古い
	オンライン	使用不可、ソースに再度接続しています	機能しています	無効	最新またはやや古い
	オンライン	使用可能	機能しています	無効	著しく古い
	オンライン	使用不可、ソースに再度接続しています	機能しています	無効	著しく古い
	オンライン	使用可能	無効または機能していません	無効または機能していません	最新またはやや古い
	オンライン	使用不可、ソースに再度接続しています	無効または機能していません	無効または機能していません	最新またはやや古い

アイコン	Apex One サーバとの接続	Trend Micro Smart Protection ソースで提供される Web レピュテーションサービス	リアルタイム検索サービス	リアルタイム検索	ウイルスパターンファイル
	オンライン	使用可能	無効または機能していません	無効または機能していません	著しく古い
	オンライン	使用不可、ソースに再度接続しています	無効または機能していません	無効または機能していません	著しく古い
	オフライン	使用可能	機能しています	有効	最新またはやや古い
	オフライン	使用不可、ソースに再度接続しています	機能しています	有効	最新またはやや古い
	オフライン	使用可能	機能しています	有効	著しく古い
	オフライン	使用不可、ソースに再度接続しています	機能しています	有効	著しく古い
	オフライン	使用可能	機能しています	無効	最新またはやや古い
	オフライン	使用不可、ソースに再度接続しています	機能しています	無効	最新またはやや古い
	オフライン	使用可能	機能しています	無効	著しく古い
	オフライン	使用不可、ソースに再度接続しています	機能しています	無効	著しく古い

アイコン	Apex One サーバとの接続	Trend Micro Smart Protection ソースで提供される Web レピュテーションサービス	リアルタイム検索サービス	リアルタイム検索	ウイルスパターンファイル
	オフライン	使用可能	無効または機能していません	無効または機能していません	最新またはやや古い
	オフライン	使用不可、ソースに再度接続しています	無効または機能していません	無効または機能していません	最新またはやや古い
	オフライン	使用可能	無効または機能していません	無効または機能していません	著しく古い
	オフライン	使用不可、ソースに再度接続しています	無効または機能していません	無効または機能していません	著しく古い
	スタンドアロン	使用可能	機能しています	有効	最新またはやや古い
	スタンドアロン	使用不可、ソースに再度接続しています	機能しています	有効	最新またはやや古い
	スタンドアロン	使用可能	機能しています	有効	著しく古い
	スタンドアロン	使用不可、ソースに再度接続しています	機能しています	有効	著しく古い
	スタンドアロン	使用可能	機能しています	無効	最新またはやや古い
	スタンドアロン	使用不可、ソースに再度接続しています	機能しています	無効	最新またはやや古い

アイコン	Apex One サーバとの接続	Trend Micro Smart Protection ソースで提供される Web レピュテーションサービス	リアルタイム検索サービス	リアルタイム検索	ウイルスパターンファイル
	スタンドアロン	使用可能	機能しています	無効	著しく古い
	スタンドアロン	使用不可、ソースに再度接続しています	機能しています	無効	著しく古い
	スタンドアロン	使用可能	無効または機能していません	無効または機能していません	最新またはやや古い
	スタンドアロン	使用不可、ソースに再度接続しています	無効または機能していません	無効または機能していません	最新またはやや古い
	スタンドアロン	使用可能	無効または機能していません	無効または機能していません	著しく古い
	スタンドアロン	使用不可、ソースに再度接続しています	無効または機能していません	無効または機能していません	著しく古い
	オンライン	なし (Web レピュテーション機能はエージェントで無効化されています)	機能しています	有効	最新またはやや古い
	オンライン	なし (Web レピュテーション機能はエージェントで無効化されています)	機能しています	有効	著しく古い

アイコン	Apex One サーバとの接続	Trend Micro Smart Protection ソースで提供される Web レピュテーションサービス	リアルタイム検索サービス	リアルタイム検索	ウイルスパターンファイル
	オンライン	なし (Web レピュテーション機能はエージェントで無効化されています)	機能しています	無効	最新またはやや古い
	オンライン	なし (Web レピュテーション機能はエージェントで無効化されています)	機能しています	無効	著しく古い
	オンライン	なし (Web レピュテーション機能はエージェントで無効化されています)	無効または機能していません	無効または機能していません	最新またはやや古い
	オンライン	なし (Web レピュテーション機能はエージェントで無効化されています)	無効または機能していません	無効または機能していません	著しく古い
	オフライン	なし (Web レピュテーション機能はエージェントで無効化されています)	機能しています	有効	最新またはやや古い
	オフライン	なし (Web レピュテーション機能はエージェントで無効化されています)	機能しています	有効	著しく古い

アイコン	Apex One サーバとの接続	Trend Micro Smart Protection ソースで提供される Web レピュテーションサービス	リアルタイム検索サービス	リアルタイム検索	ウイルスパターンファイル
	オフライン	なし (Web レピュテーション機能はエージェントで無効化されています)	機能しています	無効	最新またはやや古い
	オフライン	なし (Web レピュテーション機能はエージェントで無効化されています)	機能しています	無効	著しく古い
	オフライン	なし (Web レピュテーション機能はエージェントで無効化されています)	無効または機能していません	無効または機能していません	最新またはやや古い
	オフライン	なし (Web レピュテーション機能はエージェントで無効化されています)	無効または機能していません	無効または機能していません	著しく古い
	スタンドアロン	なし (Web レピュテーション機能はエージェントで無効化されています)	機能しています	有効	最新またはやや古い
	スタンドアロン	なし (Web レピュテーション機能はエージェントで無効化されています)	機能しています	有効	著しく古い

アイコン	Apex One サーバとの接続	Trend Micro Smart Protection ソースで提供される Web レピュテーションサービス	リアルタイム検索サービス	リアルタイム検索	ウイルスパターンファイル
	スタンドアロン	なし (Web レピュテーション機能はエージェントで無効化されています)	機能しています	無効	最新またはやや古い
	スタンドアロン	なし (Web レピュテーション機能はエージェントで無効化されています)	機能しています	無効	著しく古い
	スタンドアロン	なし (Web レピュテーション機能はエージェントで無効化されています)	無効または機能していません	無効または機能していません	最新またはやや古い
	スタンドアロン	なし (Web レピュテーション機能はエージェントで無効化されています)	無効または機能していません	無効または機能していません	著しく古い

セキュリティエージェントアイコンが示す問題の解決方法

セキュリティエージェントのアイコンが次のいずれかの状態を示している場合、必要な処理を実行します。

状態	説明
パターンファイルがしばらくアップデートされていない	セキュリティエージェントユーザはコンポーネントをアップデートする必要があります。Web コンソールから、[アップデート] > [エージェント] > [自動アップデート]の順に選択してコンポーネントのアップデートの設定を行うか、[エージェント] > [エージェント管理] > [設定] > [権限とその他の設定] > [権限] (タブ) > [コンポー

状態	説明
	ネントのアップデート] の順に選択してユーザにアップデートする権限を付与します。
リアルタイム検索が無効であるか機能していない	リアルタイム検索サービス (Apex One NT RealTime Scan) が停止しているか機能しなくなった場合は、Microsoft 管理コンソール (MMC) からサービスを手動で起動する必要があります。
リアルタイム検索が無効	Web コンソールからリアルタイム検索を有効にします ([エージェント] > [エージェント管理] > [設定] > [検索設定] > [リアルタイム検索設定])。
リアルタイム検索が無効で、セキュリティエージェントがスタンドアロンモード	ユーザは、まずスタンドアロンモードを無効にする必要があります。スタンドアロンモードを無効にしたら、Web コンソールからリアルタイム検索を有効にします。
ネットワークに接続されているセキュリティエージェントがオフラインとして表示される	Web コンソールから接続を確認し ([エージェント] > [接続状態の確認])、接続状態の確認ログをチェックします ([ログ] > [エージェント] > [接続状態の確認])。 確認後もセキュリティエージェントがオフラインになっている場合は、次の手順を実行します。 1. 接続状態が、セキュリティエージェントとサーバの両方ともオフラインの場合、ネットワーク接続をチェックします。 2. 接続状態が、セキュリティエージェント側がオフラインでサーバ側がオンラインの場合、サーバのドメイン名が変更されている可能性があり、セキュリティエージェントはそのドメイン名を使用してサーバに接続します (サーバインストール時にドメイン名を選択した場合)。Apex One サーバのドメイン名を DNS または WINS サーバに登録するか、ドメイン名および IP 情報をエージェントエンドポイントの<Windows フォルダ>¥system32¥drivers¥etc の「hosts」ファイルに追加します。 3. 接続状態が、セキュリティエージェント側がオンラインでサーバ側がオフラインの場合、Apex One のファイアウォール設定をチェックします。ファイアウォールで、サーバからエージェントへの通信をブロックし、エージェントからサーバへの通信を許可している可能性があります。 4. 接続状態が、セキュリティエージェント側がオンラインでサーバ側がオフラインの場合、セキュリティエージェントの IP アドレスが変更されている可能性がありますが、その状態

状態	説明
	はサーバに反映されません (エージェントを再ロードした場合など)。セキュリティエージェントの再配信を実行してください。
Trend Micro Smart Protection ソースが使用できない	エージェントから Trend Micro Smart Protection ソースへの接続が失われた場合は、次のタスクを実行します。 1. Web コンソールで エンドポイントの位置 画面 ([エージェント] > [エンドポイントの位置]) に移動し、エンドポイントの位置に関連する次の設定が正しく指定されているか確認します。 • 参照サーバおよびポート番号 • ゲートウェイ IP アドレス 2. Web コンソールで [Smart Protection Source] 画面 ([管理] > [Smart Protection] > [Smart Protection ソース]) に移動し、次のタスクを実行します。 a. 標準またはカスタムのソースリストの Smart Protection Server の設定に誤りがないか確認します。 b. サーバへの接続を確立できるかどうかテストします。 c. ソースリストの設定後、[すべてのエージェントに通知] をクリックします。 3. Smart Protection Server とセキュリティエージェント上の次の設定ファイルが、同期されているかどうかを確認します。 • `sscfg.ini` • `ssnotify.ini` 4. レジストリエディタを開いて、エージェントが企業ネットワークに接続されているかどうか確認します。 キー: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\iCRC Scan\Scan Server` • `LocationProfile=1` の場合、セキュリティエージェントはネットワークに接続されており、Smart Protection Server に接続できるはずです。 • `LocationProfile=2` の場合、セキュリティエージェントはネットワークに接続されておらず、Trend Micro Smart

状態	説明
	Protection Network に接続する必要があります。セキュリティエージェントエンドポイントで、Internet Explorer からインターネットの Web ページを表示できるかどうかをチェックします。 5. Trend Micro Smart Protection Network および Smart Protection Server との接続に使用する内部プロキシおよび外部プロキシの設定をチェックします。 詳細については、689 ページの「内部エージェントのプロキシ設定」および 690 ページの「外部エージェントのプロキシ設定」を参照してください。 6. 従来型スキャンエージェントで Windows 7、Server 2012、それ以降のバージョンを実行している場合は、tmusa ドライバが動作していることを確認します。このドライバが停止していると、エージェントは、Trend Micro Smart Protection ソースに接続して Web レピュテーションサービスを使用できません。

エージェントとサーバ間の接続の確認

Apex One サーバとのセキュリティエージェントの接続状態は、Apex One のエージェントツリーに表示されます。

場合によっては、エージェントツリーがセキュリティエージェントの正しい接続状態を示さないことがあります。たとえば、誤ってセキュリティエージェントエンドポイントからネットワークケーブルが抜かれると、セキュリティエージェントはオフラインになったことをサーバに通知することはできません。このセキュリティエージェントは、エージェントツリー内ではそのままオンラインとして表示されます。

セキュリティエージェントとサーバの接続を手動で確認するか、または Apex One で予約確認を実行します。特定のドメインまたはセキュリティエージェントを選択して接続状態を確認することはできません。Apex One は、登録されているすべてのセキュリティエージェントの接続状態を確認します。

エージェントとサーバ間の接続の確認

手順

1. [エージェント] > [接続状態の確認] に移動します。
2. エージェントとサーバ間の接続を手動で確認するには、[接続状態の確認] タブに移動して、[接続状態を確認する] をクリックします。
3. エージェントとサーバ間の接続を自動的に確認するには、[接続状態確認の間隔] タブに移動します。
   a. [接続状態確認の予約設定] を選択します。
   b. 確認の頻度と開始時刻を選択します。
   c. [保存] をクリックして、確認スケジュールを保存します。
4. エージェントツリーを調べて状態を確認するか、または接続状態の確認ログを確認します。

接続状態の確認ログ

Apex One に保存される接続状態の確認ログを使用して、Apex One サーバが登録されているすべてのエージェントと通信できるかどうかを確認できます。確認ログのエントリは、Web コンソールからエージェントとサーバ間の接続を確認するたびに作成されます。

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログの削除スケジュールを設定します。ログの管理方法の詳細については、616 ページの「ログ管理」を参照してください。

接続状態の確認ログの表示

手順

1. [ログ] > [エージェント] > [接続状態の確認] に移動します。

2. 接続状態の確認の結果を表示するには、[ステータス] 列をチェックします。

3. ログを CSV ファイルに保存するには、[CSV 形式ですべてエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。

到達不能エージェント

NAT ゲートウェイ背後のネットワークセグメントにあるエージェントなど、到達不能ネットワークのセキュリティエージェントにはサーバから直接接続を確立できないため、ほとんどの場合はオフラインになっています。そのため、サーバからエージェントに次の通知を実行できません。

- 最新コンポーネントのダウンロードを指示する通知。
- Web コンソールの設定をエージェントで適用することについての通知。たとえば、Web コンソールで予約検索の頻度を変更した場合、サーバからただちに新しい設定を適用するようにエージェントへ通知されます。

これにより、到達不能エージェントではこれらのタスクを適切なタイミングで実行できません。これらのタスクはサーバへの接続が開始されたときにのみ実行されます。接続は次の場合に実行されます。

- インストール後のサーバへの登録時。
- 再起動または再ロード時。このイベントの発生頻度は少なく、通常はユーザの操作が必要です。
- エージェントでの手動または予約アップデートの実行時。このイベントの発生頻度も多くはありません。

登録、再起動、または再ロードの実行時のみ、サーバはエージェントの接続を「認識」し、オンラインとして処理します。ただし、サーバからエージェントへの接続を確立することは依然としてできないため、ステータスがすぐにオフラインに変更されます。

Apex One では、到達不能エージェントの問題を解決するために、「接続ステータス」とサーバへのポーリング機能が提供されています。これらの機能では、サーバはコンポーネントのアップデートと設定の変更に関するエージェントへの通知を停止します。代わりに、受動的な処理に移行し、エージェントか

らの接続ステータスの送信や、エージェントでのポーリングの開始を常時待機します。サーバでこれらのイベントが検出されると、そのエージェントは「到達不能/オンライン」として処理されます。

注意

エージェントで発生する、接続ステータスやサーバへのポーリングに関係しないイベントには手動アップデートやログ送信などがありますが、これらのイベントによってサーバの到達不能エージェントのステータスが更新されることはありません。

接続ステータス

セキュリティエージェントは、接続ステータスメッセージを送信して、サーバにエージェントからの接続が機能していることを通知します。接続ステータスメッセージを受信したサーバは、そのエージェントをオンラインとみなします。エージェントツリーに表示されるエージェントのステータスは次のいずれかです。

- オンライン:通常のオンラインエージェントの場合
- 到達不能/オンライン:到達不能なネットワーク内にあるオンラインエージェントの場合

注意

セキュリティエージェントは、接続ステータスメッセージを送信する際、コンポーネントのアップデートや新しい設定の適用は実行されません。通常のエージェントでは、定期的なアップデート時にこれらのタスクが実行されます (231 ページの「セキュリティエージェントのアップデート」を参照)。到達不能なネットワーク内にあるエージェントでは、サーバのポーリング時にこれらのタスクが実行されます。

接続ステータス機能は、到達不能なネットワーク内にあるセキュリティエージェントがサーバに接続可能なときでもオフラインと表示される問題に対応するものです。

Web コンソールの設定で、エージェントからの接続ステータスメッセージの送信頻度を制御できます。サーバが接続ステータスを受信しなかった場合、そのエージェントはすぐにはオフラインとはみなされません。接続メッセー

ジをどれだけの期間受信しなかった場合に、エージェントのステータスを次のステータスに変更するかを Web コンソールで設定できます。

- オフライン:通常のオフラインセキュリティエージェントの場合
- 到達不能/オフライン:到達不能なネットワーク内にあるオフラインセキュリティエージェントの場合

接続ステータスの設定は、最新のエージェントステータス情報表示に関するニーズと、システムリソースの管理上のニーズのバランスを考慮して決定する必要があります。ほとんどの状況では、初期設定で十分です。接続ステータスの設定をカスタマイズする場合には、次の点を考慮してください。

表 15-11. 接続ステータスの推奨設定

接続ステータスの頻度	推奨事項
間隔の長い接続ステータス (60 分以上)	接続ステータスの間隔を長くすると、サーバの Web コンソールにエージェントのステータスが反映されるまでに発生するイベント数が多くなります。
間隔の短い接続ステータス (60 分未満)	間隔を短くすると、より最新のエージェントステータスが表示される一方、帯域幅の消費も多くなる可能性があります。

サーバへのポーリング

サーバへのポーリング機能は、到達不能セキュリティエージェントで、コンポーネントのアップデートやエージェント設定の変更に関する通知が適当なタイミングで行われない問題に対応します。これは接続ステータス機能から独立した機能です。

サーバへのポーリング機能によって、次の処理が実行されます。

- セキュリティエージェントが定期的に Apex One サーバと自動的に接続します。サーバでポーリングの実行が検出されると、そのエージェントは「到達不能/オンライン」として処理されます。
- セキュリティエージェントは、1 つまたは複数のアップデートソースに接続し、最新コンポーネントのダウンロードや新しいエージェント設定の適用を実行します。Apex One サーバまたはアップデートエージェントが 1 次アップデート元の場合、エージェントはコンポーネントと新しい設定の両方を取得します。アップデート元が Apex One サーバやアップ

デートエージェントでない場合、エージェントは最新コンポーネントのみを取得し、次に Apex One サーバまたはアップデートエージェントに接続して新しい設定を取得します。

接続ステータスおよびサーバポーリング機能の設定

手順

1. [エージェント] > [グローバルエージェント設定] に移動します。
2. [ネットワーク] タブをクリックします。
3. [到達不能ネットワーク] セクションに移動します。
4. サーバへのポーリング設定を指定します。

   サーバへのポーリングの詳細については、684 ページの「サーバへのポーリング」を参照してください。

   a. Apex One サーバが IPv4 と IPv6 の両方のアドレスを持っている場合は、IPv4 のアドレス範囲と IPv6 のプレフィックスおよび長さを入力できます。

      サーバが IPv4 シングルスタックの場合は IPv4 のアドレス範囲を入力し、IPv6 シングルスタックの場合は IPv6 のプレフィックスおよび長さを入力します。

      あるエージェントの IP アドレスがこの範囲の IP アドレスと一致する場合、エージェントでは接続状態とサーバポーリング設定が適用され、サーバではそのエージェントが到達不能ネットワーク内に存在するものとして処理されます。

注意

IPv4 アドレスを持つエージェントは、IPv4 シングルスタックまたはデュアルスタックの Apex One サーバに接続できます。

IPv6 アドレスを持つエージェントは、IPv6 シングルスタックまたはデュアルスタックの Apex One サーバに接続できます。

デュアルスタックエージェントは、デュアルスタック、IPv4 シングルスタック、または IPv6 シングルスタックの Apex One サーバに接続できます。

b. [コンポーネントと設定の最新情報を確認するため、エージェントで__分ごとにサーバのポーリングを実行] に、サーバのポーリング間隔を指定します。1～129,600 の値を入力します。

ヒント

サーバポーリングの間隔は、接続ステータスの送信間隔の 3 倍以上に設定することをお勧めします。

5. 接続ステータスの設定を指定します。

接続ステータス機能の詳細については、683 ページの「接続ステータス」を参照してください。

a. [エージェントからサーバへの接続ステータスの送信を許可] を選択します。

b. [すべてのエージェント] または [到達不能ネットワーク内のエージェントのみ] を選択します。

c. [エージェントから__分ごとに接続ステータスを送信] に、エージェントからの接続ステータスの送信間隔を指定します。1～129,600 の値を入力します。

d. [接続ステータスが__分間送信されない場合はエージェントをオフラインと判断] に、接続ステータス受信なしの持続時間を指定します。受信がないままこの時間が経過すると、Apex One サーバはエージェントをオフラインとして処理します。1～129,600 の値を入力します。

6. [保存] をクリックします。

セキュリティエージェントプロキシ設定

次の表は、セキュリティエージェントが内部サーバおよび外部サーバへの接続にプロキシを使用する場合に必要なプロキシ設定の説明です。

プロキシ設定	説明
内部エージェント	次のサーバに接続するための内部エージェントのプロキシ設定を行います。 • Apex One サーバ: サーバコンピュータは、Apex One サーバおよび統合 Smart Protection Server をホストします。セキュリティエージェントは Apex One サーバに接続して、コンポーネントのアップデート、設定の取得、およびログの送信を行います。セキュリティエージェントは統合 Smart Protection Server に接続して、検索クエリを送信します。 • Smart Protection Server: Smart Protection Server には、すべてのスタンドアロンの Smart Protection Server、および別の Apex One サーバの統合 Smart Protection Server が含まれます。セキュリティエージェントはサーバに接続して、検索クエリと Web レピュテーションクエリを送信します。 詳細については、689 ページの「内部エージェントのプロキシ設定」を参照してください。
外部エージェント	外部セキュリティエージェントは、Internet Explorer で設定されたプロキシ設定を使用して、Trend Micro Smart Protection Network に接続します。 詳細については、690 ページの「外部エージェントのプロキシ設定」を参照してください。

プロキシ設定	説明
Global Smart Protection サービス	セキュリティエージェントは、次の機能で Smart Protection ソースに対してクエリを実行するとき、設定されている Smart Protection サービスプロキシ設定を使用します。 • 機械学習型検索 • 挙動監視 **注意** 統合 Smart Protection Server を使用できない場合、セキュリティエージェントはクエリの実行時に Trend Micro Smart Protection Network に接続します。 詳細については、691 ページの「グローバル Smart Protection サービスプロキシ設定」を参照してください。
エージェントユーザのプロキシ権限	各エージェント毎に、プロキシ設定をエージェントコンソールにて実施する権限を付与できます。各セキュリティエージェント毎に、エージェントコンソールにて設定したプロキシ設定は、次の場合に使用されます。 • セキュリティエージェントで「今すぐアップデート」が実行された場合。 • ユーザが自動プロキシ設定を無効にした場合、またはセキュリティエージェントで自動プロキシ設定を検出できない場合。 **警告!** ユーザによるプロキシ設定に誤りがあると、アップデート時に問題が発生することがあります。プロキシ設定権限をユーザに付与する際には、注意するよう指示してください。 詳細については、692 ページの「プロキシ設定権限の付与」を参照してください。

内部エージェントのプロキシ設定

手順

1. [管理] > [設定] > [プロキシ] に移動します。
2. [エージェント] タブを選択します。
3. [内部プロキシ] に移動します。
4. 内部のセキュリティエージェントが Apex One サーバまたは Smart Protection Server への接続時に使用するプロキシ設定の種類を選択します。
   - プロキシなし: 内部のセキュリティエージェントは、Apex One サーバまたは Smart Protection Server への接続時にプロキシサーバを必要としません。
   - Windows のプロキシ設定を使用する: 内部エージェントは、Apex One サーバまたは Smart Protection Server への接続時に Windows の [インターネット オプション] のプロキシサーバ設定を使用します。

     注意
     必要に応じて、プロキシの認証アカウント情報を指定してください。
   - 複数のプロキシサーバを使用する: 内部エージェントは、Apex One サーバまたは Smart Protection Server への接続時に複数のプロキシサーバを使用します。

     Apex One サーバに接続するには、次の手順を実行します。

     a. [Apex One サーバに接続する際に、次のプロキシ設定を使用する] を選択します。
     b. プロキシサーバの名前または IPv4/IPv6 アドレス、およびポート番号を指定します。
     c. 必要に応じて、プロキシの認証アカウント情報を指定してください。

スタンドアロンの Smart Protection Server に接続するには、次の手順を実行します。

a. [スタンドアロンの Smart Protection Server に接続する際に、次のプロキシ設定を使用する] を選択します。

b. プロキシサーバの名前または IPv4/IPv6 アドレス、およびポート番号を指定します。

c. 必要に応じて、プロキシの認証アカウント情報を指定してください。

- 自動プロキシ設定 (PAC を含む) を使用する: DHCP、DNS、または自動設定スクリプトを使用した、管理者指定のプロキシ設定を使用する場合に選択します。
  - ネットワークプロキシ設定を自動で検出する: DHCP または DNS によって、内部エージェントが管理者指定のプロキシ設定を検出します。
  - 指定されたプロキシ自動設定 (PAC) スクリプトファイルを使用する: ネットワーク管理者が設定したプロキシ自動設定 (PAC) スクリプトを使用して、内部エージェントが適切なプロキシサーバを検出します。

注意

PAC スクリプトの URL アドレスを入力します。

5. [保存] をクリックします。

外部エージェントのプロキシ設定

外部エージェントは、Apex One サーバまたは Smart Protection Server への接続時に Windows の [インターネット オプション] のプロキシサーバ設定だけを使用できます。

手順

1. [管理] > [設定] > [プロキシ] に移動します。
2. [エージェント] タブを選択します。
3. [外部プロキシ] に移動します。
4. 必要に応じて、プロキシの認証アカウント情報を指定してください。
5. [保存] をクリックします。

グローバル Smart Protection サービスプロキシ設定

セキュリティエージェントは、次の機能で Smart Protection ソースに対してクエリを実行するとき、設定されている Smart Protection サービスプロキシ設定を使用します。

- 機械学習型検索
- 挙動監視

注意

統合 Smart Protection Server を使用できない場合、セキュリティエージェントはクエリの実行時に Trend Micro Smart Protection Network に接続します。

手順

1. [エージェント] > [グローバルエージェント設定] に移動します。
2. [システム] タブをクリックします。
3. [Smart Protection サービスプロキシ] に移動します。
4. [設定した Smart Protection ソースをサービスプロキシクエリに使用する] を有効にします。

重要

Smart Protection サービスプロキシでファイルレピュテーションクエリにサポートされるのは、HTTPS プロトコルのみです。ファイルレピュテーションサービスを提供する設定済みのすべての Smart Protection Server で HTTPS プロトコルを使用するようにしてください。

初期設定では、統合 Smart Protection Server は HTTPS 通信を使用しません。通信方法を変更するには、122 ページの「統合 Smart Protection Server の設定」を参照してください。

スタンドアロンの Smart Protection Server で使用されている通信方法を確認するには、128 ページの「Trend Micro Smart Protection ソースのカスタムリストを設定する」を参照してください。

5. [保存] をクリックします。

プロキシ設定権限の付与

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [権限] タブの [プロキシ設定] セクションに移動します。
5. [ユーザにプロキシの設定を許可] を選択します。
6. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。
   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。

- 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

セキュリティエージェントの情報の表示

[ステータスの表示] 画面には、権限、エンドポイントソフトウェアの詳細、システムイベントなど、セキュリティエージェントに関する重要な情報が表示されます。

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [ステータス] をクリックします。
4. ステータス情報を表示するには、対象のエージェントエンドポイント名を展開します。複数のエージェントを選択した場合、[すべて展開する] をクリックすると、選択したすべてのエージェントのステータス情報が表示されます。
5. (オプション) [リセット] ボタンを使用して、セキュリティリスクのカウントを 0 に戻すことができます。

エージェント設定のインポートとエクスポート

Apex One では、特定のセキュリティエージェントまたはドメインによって適用されたエージェントツリー設定をファイルにエクスポートできます。その後、このファイルをインポートすることによって、他のエージェント、ドメイン、および同じバージョンの別の Apex One サーバに設定を適用できます。

エージェントツリーの、アップデートエージェント設定を除くすべての設定がエクスポートされます。

エージェント設定のエクスポート

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [設定のエクスポート] の順にクリックします。
4. 任意のリンクをクリックして、選択したセキュリティエージェントまたはドメインの設定を表示します。
5. [エクスポート] をクリックして、設定を保存します。

   設定は.dat ファイルに保存されます。
6. [保存] をクリックして、.dat ファイルの保存先を指定します。
7. [保存] をクリックします。

エージェント設定のインポート

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [設定のインポート] の順にクリックします。

4. [参照] をクリックしてエンドポイント上で.dat ファイルを探し、[インポート] をクリックします。

   [設定のインポート] 画面が開き、設定の概要が表示されます。

5. インポートする検索設定または権限のリンクをクリックして、設定の詳細を表示します。

6. 設定をインポートします。

   - ルートドメインアイコンをクリックした場合は、[すべてのドメインに適用する] を選択して [適用] をクリックします。
   - ドメインを選択した場合は、[選択したドメインに属するすべてのコンピュータに適用する] を選択して [適用] をクリックします。
   - 複数のエージェントを選択した場合は、[適用] をクリックします。

セキュリティコンプライアンス

セキュリティコンプライアンスを使用して、脆弱箇所の特定、ソリューションの配信、セキュリティ基盤の維持を行うことができます。この機能は、ネットワーク環境のセキュリティの維持に要する時間を削減し、組織におけるセキュリティと機能の要求のバランスを保つのに役立ちます。

次の 2 種類のエンドポイントに対してセキュリティコンプライアンスを適用します。

- 管理対象:Apex One サーバによって管理されるセキュリティエージェントがインストールされたエンドポイント。詳細については、696 ページの「管理対象エージェントのセキュリティコンプライアンス」を参照してください。
- 管理対象外:次のものが含まれます。
  - Apex One サーバによって管理されていないセキュリティエージェント。
  - セキュリティエージェントがインストールされていないエンドポイント。

- Apex One サーバからアクセスできないエンドポイント。
- セキュリティステータスを確認できないエンドポイント。

  詳細については、707 ページの「管理対象外のエンドポイントに関するセキュリティコンプライアンス」を参照してください。

管理対象エージェントのセキュリティコンプライアンス

セキュリティコンプライアンスで生成されるコンプライアンスレポートは、Apex One サーバの管理対象セキュリティエージェントのセキュリティステータスを診断するのに役立ちます。セキュリティコンプライアンスレポートは、手動で生成するか、予約設定によって生成されます。

注意

Apex One のコンプライアンスレポートの対象となるのは、すべての機能を備えたフル機能のセキュリティエージェントだけです。限定機能モードのエージェントはレポートに表示されません。

[手動コンプライアンスレポート] 画面には次のタブが表示されます。

- サービス:このタブでは、エージェントサービスが機能しているかどうか確認できます。

  詳細については、697 ページの「サービス」を参照してください。
- コンポーネント:このタブでは、セキュリティエージェントのコンポーネントが最新のものかどうか確認できます。

  詳細については、698 ページの「コンポーネント」を参照してください。
- 検索:このタブでは、セキュリティエージェントが検索を定期的に実行しているかどうか確認できます。

  詳細については、700 ページの「検索」を参照してください。
- 設定:このタブでは、エージェントの設定がサーバ上の設定と一致しているかどうか確認できます。

  詳細については、701 ページの「設定」を参照してください。

注意

[コンポーネント] タブでは、最新バージョンまたは旧バージョンのいずれかを実行しているセキュリティエージェントを表示できます。その他のタブには、最新バージョンを実行しているセキュリティエージェントのデータのみが表示されます。

重要

- セキュリティコンプライアンスでは、コンプライアンスレポートの生成前にセキュリティエージェントの接続状態に関するクエリが実行されます。レポートには、オンラインエージェントとオフラインエージェントが含まれますが、スタンドアロンエージェントは含まれません。
- 役割ベースのユーザアカウントの場合:
  - コンプライアンスレポートの設定は、Web コンソールのユーザアカウントごとに完全に独立しています。あるユーザアカウントでコンプライアンスレポートの設定を変更しても、他のユーザアカウントの設定には影響しません。
  - レポートの範囲は、ユーザアカウントのエージェントドメイン権限に依存します。たとえば、あるユーザアカウントにドメイン A および B を管理する権限を付与した場合、このユーザアカウントのレポートには、ドメイン A および B に属するエージェントのデータのみが表示されます。

    ユーザアカウントの詳細については、575 ページの「役割ベースの管理」を参照してください。

サービス

セキュリティコンプライアンスによって、次のセキュリティエージェントサービスが機能しているかどうかが確認できます。

- ウイルス対策
- スパイウェア対策
- ファイアウォール
- Web レピュテーション

- 挙動監視/デバイスコントロール (別名: Trend Micro Unauthorized Change Prevention Service)
- 情報漏えい対策オプション
- 不審接続監視

コンプライアンス違反のエージェントはコンプライアンスレポートで少なくとも 2 回カウントされます。

- [非準拠サービスが存在するエンドポイント] でカウントされます。
- さらに、そのセキュリティエージェントのコンプライアンス違反が検出されたカテゴリでカウントされます。たとえば、セキュリティエージェントでウイルス対策サービスが機能していない場合、そのエージェントは [ウイルス対策] カテゴリでカウントされます。機能していないサービスが複数検出された場合、そのエージェントは非準拠のカテゴリごとにそれぞれカウントされます。

Web コンソールまたはセキュリティエージェントから、機能していないサービスを再起動します。再起動後にサービスが機能している場合、次の診断では、そのエージェントは非準拠として表示されません。

コンポーネント

セキュリティコンプライアンスによって、Apex One サーバとセキュリティエージェントとの間で一致しないコンポーネントが特定されます。この不一致は通常、エージェントが、コンポーネントをアップデートするためにサーバに接続できない場合に発生します。このとき、エージェントが別のアップデート元 (トレンドマイクロのアップデートサーバなど) からアップデートを取得する場合、エージェントのコンポーネントのバージョンがサーバ上のバージョンよりも新しくなることがあります。

セキュリティコンプライアンスによってチェックされるコンポーネントは次のとおりです。

- スマートスキャンエージェントパターンファイル
- ウイルスパターンファイル
- IntelliTrap パターンファイル
- IntelliTrap 除外パターンファイル
- ウイルス検索エンジン (32/64 ビット)
- スパイウェア/グレーウェアパターンファイル
- スパイウェア監視パターンファイル
- スパイウェア検索エンジン (32/64 ビット)
- ダメージクリーンナップテンプレート
- ダメージクリーンナップエンジン (32 ビット/64 ビット)
- ファイアウォールパターンファイル
- ファイアウォールドライバ (32/64 ビット)
- 挙動監視コアドライバ (32 ビット/64 ビット)
- 挙動監視コアサービス (32 ビット/64 ビット)
- 挙動監視設定パターンファイル
- デジタル署名パターンファイル
- ポリシー施行パターンファイル
- 挙動監視検出パターンファイル (32 ビット/64 ビット)
- グローバル C&C IP リスト
- 適合度ルールパターンファイル
- 起動時クリーンナップドライバ (32/64 ビット)
- メモリ検索実行パターンファイル (32 ビット/64 ビット)
- メモリ検査パターンファイル
- ブラウザ脆弱性対策パターンファイル
- スクリプトアナライザ共通パターンファイル
- プログラム検査監視パターンファイル
- ダメージリカバリパターンファイル
- ELAM パターンファイル (32/64 ビット)
- CI エンジン (32/64 ビット)
- CI パターンファイル
- CI クエリハンドラ (32/64 ビット)
- 高度な脅威検索エンジン (32/64 ビット)
- 高度な脅威相関パターンファイル
- プログラムバージョン

コンプライアンス違反のエージェントはコンプライアンスレポートで少なくとも 2 回カウントされます。

- [コンポーネントのバージョンが一致しないエンドポイント] カテゴリでカウントされます。
- さらに、そのエージェントのコンプライアンス違反が検出されたカテゴリでカウントされます。たとえば、エージェントのスマートスキャンエージェントパターンファイルのバージョンがサーバ上のバージョンと

一致しない場合、そのエージェントは [スマートスキャンエージェントパターンファイル] カテゴリでカウントされます。コンポーネントバージョンの不一致が複数検出された場合、そのエージェントはコンプライアンス違反のカテゴリごとにカウントされます。

コンポーネントバージョンの不一致を解決するには、エージェントまたはサーバ上の古いコンポーネントをアップデートします。

検索

セキュリティコンプライアンスによって、ScanNow または予約検索が定期的に実行されているかどうか、およびこれらの検索が妥当な時間内に完了しているかどうかがチェックされます。

注意

予約検索の状態については、エージェントで予約検索が有効化されている場合にのみレポートされます。

セキュリティコンプライアンスでは、次の検索コンプライアンス条件が使用されます。

- ScanNow または予約検索が、過去 (x) 日間実行されていません:指定された日数の間、ScanNow または予約検索が実行されていないと、そのセキュリティエージェントは非準拠として検出されます。
- ScanNow または予約検索が (x) 時間を超えました:最後に行われた ScanNow または予約検索の継続時間が指定された時間を超えている場合、そのセキュリティエージェントは非準拠として検出されます。

コンプライアンス違反のエージェントはコンプライアンスレポートで少なくとも 2 回カウントされます。

- [検索が必要なコンピュータ] カテゴリでカウントされます。
- さらに、そのエージェントのコンプライアンス違反が検出されたカテゴリでカウントされます。たとえば、最後に行われた予約検索の継続時間が指定された時間を超えている場合、そのエージェントは [ScanNow または予約検索が (x) 時間を超えました] カテゴリでカウントされます。検索コンプライアンス条件への一致が複数検出された場合、そのエージェントは非準拠のカテゴリごとにそれぞれカウントされます。

検索タスクが実行されていないか、検索を完了できなかったエージェントで、ScanNow または予約検索を実行します。

設定

セキュリティコンプライアンスによって、エージェントツリー内のエージェントとその親ドメインの設定が一致しているかどうかが判定されます。エージェントを移動し、移動先のドメインに元のドメインとは異なる設定が適用されている場合や、特定の権限を持つエージェントユーザがセキュリティエージェントコンソールで手動で設定を行った場合、設定の不一致が発生することがあります。

Apex One は次の設定を検証します。

- **検索方法**
- **手動検索の設定**
- **リアルタイム検索の設定**
- **予約検索の設定**
- ScanNow の設定
- **権限とその他の設定**
- **追加サービス設定**
- Web レピュテーション
- **挙動監視**
- **デバイスコントロール**
- **スパイウェア/グレーウェアの承認済みリスト**
- **情報漏えい対策設定**
- **不審接続監視**
- **信頼済みプログラムリスト**
- **サンプル送信**
- **機械学習型検索**

コンプライアンス違反のエージェントはコンプライアンスレポートで少なくとも 2 回カウントされます。

- [設定に矛盾があるエンドポイント] カテゴリでカウントされます。
- さらに、そのエージェントのコンプライアンス違反が検出されたカテゴリでカウントされます。たとえば、エージェントとその親ドメインとの間で検索方法の設定が一致していない場合、そのエージェントは [検索方法] カテゴリでカウントされます。設定の不一致が複数検出された場合、そのエージェントは非準拠のカテゴリごとにそれぞれカウントされます。

設定の不一致を解決するには、ドメインの設定をエージェントに適用します。

手動コンプライアンスレポート

セキュリティコンプライアンス機能では、手動でコンプライアンスレポートを生成できます。レポートは、Apex One サーバの管理対象セキュリティエージェントのセキュリティステータスの診断に役立ちます。

コンプライアンスレポートの詳細については、696 ページの「管理対象エージェントのセキュリティコンプライアンス」を参照してください。

手動コンプライアンスレポートの生成

手順

1. [診断] > [セキュリティコンプライアンス] > [手動レポート]に移動します。
2. [エージェントツリー範囲] セクションに移動します。
3. ルートドメインまたはドメインを選択して [診断] をクリックします。
4. エージェントサービスに関するコンプライアンスレポートの内容を確認します。

   エージェントサービスの詳細については、697 ページの「サービス」を参照してください。

   a. [サービス] タブをクリックします。

   b. [非準拠サービスが存在するエンドポイント] で、非準拠サービスが存在するエージェント数を確認します。

   c. 数字のリンクをクリックし、エージェントツリーで影響を受けるすべてのエージェントを表示します。

   d. クエリ結果からエージェントを選択します。

   e. [セキュリティエージェントの再起動] をクリックして、サービスを再起動します。

注意

もう一度診断を実行して、それでもエージェントが非準拠として表示される場合は、そのエージェントエンドポイントでサービスを手動で再起動します。

f. エージェントのリストをファイルに保存するには、[エクスポート] をクリックします。

5. エージェントコンポーネントに関するコンプライアンスレポートの内容を確認します。

   エージェントコンポーネントの詳細については、698 ページの「コンポーネント」を参照してください。

   a. [コンポーネント] タブをクリックします。

   b. [コンポーネントのバージョンが一致しないエンドポイント] で、コンポーネントのバージョンがサーバ上のバージョンと一致しないエージェント数を確認します。

   c. 数字のリンクをクリックし、エージェントツリーで影響を受けるすべてのエージェントを表示します。

   注意

   少なくとも 1 つのエージェントで、Apex One サーバにあるコンポーネントより新しいものが検出された場合は、Apex One サーバを手動でアップデートします。

   d. クエリ結果からエージェントを選択します。

   e. [今すぐアップデート] をクリックして、エージェントでコンポーネントをダウンロードします。

注意

- エージェントでエージェントプログラムをバージョンアップできるようにするには、次の手順を実行します。
  i. [エージェント] > [エージェント管理]に移動します。
  ii. [設定] > [権限とその他の設定] > [その他の設定] タブをクリックします。
  iii. [アップデート設定] に移動します。
  iv. [セキュリティエージェントがアップデートするコンポーネント] リストで、[すべてのコンポーネント (HotFix とエージェントプログラムを含む)] を選択します。
  v. [すべてのエージェントに適用] をクリックします。
- [今すぐアップデート] をクリックする代わりにエンドポイントを再起動して、ファイアウォールドライバをアップデートします。

f. エージェントのリストをファイルに保存するには、[エクスポート] をクリックします。

6. 検索に関するコンプライアンスレポートの内容を確認します。

   検索の詳細については、700 ページの「検索」を参照してください。

   a. [検索] タブをクリックします。

   b. [検索が必要なコンピュータ] で、次の設定を指定します。

      - エージェントが ScanNow または予約検索を実行しなかった日数
      - ScanNow または予約検索が実行された時間数

      注意

      日数または時間数が上限を超えていると、そのエージェントは非準拠として扱われます。

   c. [エージェントツリー範囲] の横にある [診断] をクリックします。

   d. [検索が必要なコンピュータ] で、検索条件に一致するエージェント数をチェックします。

e. 数字のリンクをクリックし、エージェントツリーで影響を受けるすべてのエージェントを表示します。

f. クエリ結果からエージェントを選択します。

g. [ScanNow] をクリックして、エージェントで ScanNow を起動します。

注意

ScanNow の継続時間が指定された時間を超えた場合、検索の繰り返しを防ぐため、[ScanNow] オプションは無効化されます。

h. エージェントのリストをファイルに保存するには、[エクスポート] をクリックします。

7. 設定に関するコンプライアンスレポートの内容を確認します。

設定の詳細については、701 ページの「設定」を参照してください。

a. [設定] タブをクリックします。

b. [設定に矛盾があるエンドポイント] で、設定がエージェントツリードメインの設定と一致しないエージェント数をチェックします。

c. 数字のリンクをクリックし、エージェントツリーで影響を受けるすべてのエージェントを表示します。

d. クエリ結果からエージェントを選択します。

e. [ドメイン設定の適用] をクリックします。

f. エージェントのリストをファイルに保存するには、[エクスポート] をクリックします。

予約コンプライアンスレポート

セキュリティコンプライアンス機能では、コンプライアンスレポートを予約設定によって生成できます。レポートは、Apex One サーバの管理対象セキュリティエージェントのセキュリティステータスの診断に役立ちます。

コンプライアンスレポートの詳細については、696 ページの「管理対象エージェントのセキュリティコンプライアンス」を参照してください。

予約コンプライアンスレポートの設定

手順

1. [診断] > [セキュリティコンプライアンス] > [予約レポート] に移動します。
2. [予約レポートの有効化] を選択します。
3. レポートのタイトルを指定します。
4. 次のいずれか 1 つまたはすべてを選択します。
   - 697 ページの「サービス」
   - 698 ページの「コンポーネント」
   - 700 ページの「検索」
   - 701 ページの「設定」
5. 予約コンプライアンスレポートに関する通知を受信するメールアドレスを指定します。

   注意

   メール通知を正常に送信できるように、メール通知設定を指定します。詳細については、612 ページの「管理者通知設定」を参照してください。
6. スケジュールを指定します。
7. [保存]をクリックします。

管理対象外のエンドポイントに関するセキュリティコンプライアンス

セキュリティコンプライアンス機能では、Apex One サーバが属しているネットワーク内の管理対象外のエンドポイントに関するクエリを実行できます。エンドポイントのクエリには、Active Directory と IP アドレスを使用します。

管理対象外のエンドポイントのセキュリティステータスは、次のいずれかになります。

表 15-12. 管理対象外のエンドポイントのセキュリティステータス

ステータス	説明
他の Apex One サーバの管理下	コンピュータにインストールされているセキュリティエージェントは、他の Apex One サーバによって管理されています。セキュリティエージェントはオンラインで、この Apex One のバージョンかそれ以前のバージョンを実行しています。
セキュリティエージェントが未インストール	エンドポイントにはセキュリティエージェントがインストールされていません。
到達不能	Apex One サーバは、エンドポイントに接続できず、セキュリティステータスを特定できません。
未解決の Active Directory 診断	エンドポイントは Active Directory ドメインに属していますが、Apex One サーバはそのセキュリティステータスを特定できません。 **注意** Apex One サーバのデータベースには、そのサーバで管理しているエージェントのリストがあります。サーバは、Active Directory でコンピュータの GUID をクエリして、それをデータベース内の GUID と比較します。GUID がデータベースにない場合、そのエンドポイントは [未解決の Active Directory 診断] カテゴリに分類されます。

セキュリティを診断するには、次のタスクを実行します。

1. クエリの範囲を定義します。詳細については、708 ページの「Active Directory/IP アドレス範囲とクエリの定義」を参照してください。

2. クエリの結果で、保護されていないコンピュータを確認します。詳細については、710 ページの「クエリ結果の表示」を参照してください。

3. セキュリティエージェントをインストールします。詳細については、189 ページの「セキュリティコンプライアンスを使用したインストール」を参照してください。

4. 予約クエリを設定します。詳細については、712 ページの「予約クエリ診断の設定」を参照してください。

Active Directory/IP アドレス範囲とクエリの定義

クエリをはじめて使用する場合は、Active Directory/IP アドレスの範囲を定義します。この範囲には、Apex One サーバで必要に応じてまたは定期的にクエリを実行する Active Directory オブジェクトや IP アドレスを含めます。対象範囲を定義したら、クエリ処理を開始します。

注意

Active Directory の範囲を定義するため、まず Apex One を Active Directory と統合する必要があります。統合の詳細については、59 ページの「Active Directory 統合」を参照してください。

手順

1. [診断] > [管理対象外のエンドポイント] に移動します。
2. [Active Directory/IP アドレス範囲] セクションで [範囲の定義] をクリックします。

   新しい画面が表示されます。
3. Active Directory の範囲を定義するには
   a. [Active Directory の範囲] セクションに移動します。
   b. [手動診断を使用する] を選択してリアルタイムクエリを実行し、より正確な結果を取得します。このオプションを無効にした場合、Apex One のクエリ対象は、各セキュリティエージェントではなくデータベースになります。データベースのみのクエリでは処理が高速になりますが精度が低下します。

c. クエリ対象のオブジェクトを選択します。はじめてクエリを実行する場合は、1,000 アカウント未満のオブジェクトを選択して、クエリの完了にかかった時間を記録してください。このデータをパフォーマンスベンチマークとして使用します。

4. IP アドレスの範囲を定義するには

   a. [IP アドレス範囲] セクションに移動します。

   b. [IP アドレス範囲を有効にする] を選択します。

   c. IP アドレスの範囲を指定します。プラスボタンまたはマイナスボタンをクリックして、IP アドレス範囲を追加または削除します。

   - IPv4 シングルスタックの Apex One サーバでは、IPv4 のアドレス範囲を入力します。
   - IPv6 シングルスタックの Apex One サーバでは、IPv6 のプレフィックスおよび長さを入力します。
   - デュアルスタックの Apex One サーバでは、IPv4 のアドレス範囲、IPv6 のプレフィックスと長さ、またはこれらの両方を入力します。

     IPv6 のアドレス範囲の制限は、IPv4 のアドレス範囲の制限と同じ 16 ビットです。このため、プレフィックスの長さは 112～128 の間にしてください。

     表 15-13. プレフィックスの長さと IPv6 アドレスの数

長さ	IPv6 アドレスの数
128	2
124	16
120	256
116	4,096
112	65,536

5. [詳細設定] で、Apex One サーバでエージェントとの通信に使用するポートを指定します。

   Apex One サーバで使用される通信ポートを確認するには、[エージェント] > [エージェント管理] に移動してドメインを選択します。ポートは、

[IP アドレス] 列の横に表示されます。参照用にポート番号を記録しておくことをお勧めします。

a. [ポートの指定] をクリックします。

b. ポート番号を入力して [追加] をクリックします。目的のポート番号がすべて追加されるまで、このステップを繰り返します。

c. [保存]をクリックします。

6. 特定のポート番号を指定してエンドポイントの接続を確認するには、[次のポートを確認することでエンドポイントを到達不能として宣言する: <x>] チェックボックスをオンにします。接続を確立できない場合、Apex One はそのエンドポイントを到達不能としてただちに処理します。初期設定のポート番号は 135 です。

   この設定を有効にすることで、クエリを迅速に行えるようになります。これは、あるエンドポイントとの接続を確立できない場合に、Apex One サーバが他のすべての接続状態の確認タスクを実行した上でエンドポイントを到達不能として処理する必要がなくなるためです。

7. 範囲を保存してクエリを開始するには、[保存および再診断] をクリックします。設定の保存のみを実行するには、[保存のみ] をクリックします。

   [外部サーバ管理] 画面にクエリの結果が表示されます。

注意

特にクエリ範囲が広い場合、クエリの完了に時間がかかる場合があります。[外部サーバ管理] 画面に結果が表示されるまで、別のクエリは実行しないでください。結果が表示される前に別のクエリを実行すると、現在のクエリセッションが終了し、クエリ処理が再度開始されます。

クエリ結果の表示

クエリの結果は [セキュリティステータス] セクションに表示されます。管理対象外のエンドポイントは、次のいずれかのステータスになります。

- 他の Apex One サーバの管理下

- セキュリティエージェントが未インストール
- 到達不能
- 未解決の Active Directory 診断

手順

1. [セキュリティステータス] セクションで、数字のリンクをクリックし、影響を受けるすべてのコンピュータを表示します。
2. 検索および詳細検索機能を使用して、条件に一致するコンピュータのみを検索して表示します。

   詳細検索機能を使用する場合は、次の項目を指定します。

   - IPv4 のアドレス範囲
   - IPv6 のプレフィックスおよび長さ (プレフィックスは 112 から 128 の間にします)
   - エンドポイント名
   - Apex One サーバ
   - Active Directory ツリー
   - セキュリティステータス

   名前が完全でない場合、結果は返されません。完全な名前が不明な場合は、ワイルドカード文字 (*) を使用してください。
3. コンピュータのリストをファイルに保存するには、[エクスポート] をクリックします。
4. 他の Apex One サーバによって管理されているセキュリティエージェントを、現在の Apex One サーバで管理するには、エージェント移動ツールを使用します。このツールの詳細については、660 ページの「エージェント移動ツール」を参照してください。

予約クエリ診断の設定

セキュリティガイドラインが確実に適用されるように、Active Directory と IP アドレスの定期的なクエリを実行するよう Apex One サーバを設定します。

手順

1. [診断] > [管理対象外のエンドポイント] に移動します。
2. エージェントツリーの上部にある [スケジュールの定義] をクリックします。
3. 予約クエリを有効にします。
4. スケジュールを指定します。
5. [保存] をクリックします。

Trend Micro VDI オプション

Trend Micro VDI オプションを使用して、仮想デスクトップ保護を最適化します。この機能によって、単一の仮想サーバに配置されたセキュリティエージェント上のタスクを制御できます。

単一のサーバ上で複数のデスクトップを実行し、オンデマンドの検索やコンポーネントのアップデートを実行すると、大量のシステムリソースが消費されます。この機能を使用して、複数のエージェントが検索やコンポーネントのアップデートを同時に実行するのを禁止することができます。

たとえば、VMware vCenter サーバにセキュリティエージェントを実行する 3 つの仮想デスクトップがある場合、Apex One では、3 つのエージェントすべてに対して同時に ScanNow を開始し、アップデートを配信できます。Trend Micro VDI オプションは、これらのエージェントが同じ物理サーバ上に存在していることを認識し、最初のエージェントでのタスクの実行を許可し、他の 2 つのエージェントでの同じタスクの実行を最初のエージェントでタスクが完了するまで延期します。

Trend MicroVDI オプションは次のプラットフォームで使用できます。

- VMware vCenter™ (VMware View™)
- Citrix™ XenServer™ (Citrix XenDesktop™)
- Microsoft Hyper-V™ Server

他の仮想アプリケーションを使用する管理者向けに、Apex One サーバは仮想エージェントを管理するエミュレートハイパーバイザとして機能することもできます。

オンデマンドの検索を最適化したり、ベースまたはゴールドイメージから GUID を削除するには、Apex One VDI 事前検索テンプレート生成ツールを使用します。

Trend Micro VDI オプションのシステム要件

システム要件の完全なリストについては、次の Web サイトを参照してください。

http://www.go-tm.jp/corp/req

Trend Micro VDI オプションのインストール

Trend Micro VDI オプションは Apex One のデフォルトの機能ですが、ライセンスは別途必要です。Apex One サーバをインストールすると、この機能が利用可能になりますが、まだ機能していません。この機能のインストールは、設定が完了しているトレンドマイクロのアップデートサーバまたはユーザ指定のアップデート元からファイルをダウンロードすることを意味します。このファイルの Apex One サーバへの組み込みを完了すれば、Trend Micro VDI オプションをアクティベートしてその機能のすべてを有効にすることができます。インストールとアクティベーションはプラグインマネージャから実行します。

注意

Trend Micro VDI オプションは、IPv6 シングルスタックの環境には完全対応していません。詳細については、808 ページの「IPv6 シングルスタックサーバの制限事項」を参照してください。

Trend Micro VDI オプションのインストール

手順

1. Apex One Web コンソールを開いて、メインメニューで [プラグイン] をクリックします。
2. [プラグインマネージャ] 画面で、[Trend Micro VDI オプション] セクションに移動し、[ダウンロード] をクリックします。

   パッケージのサイズは、[ダウンロード] ボタンの横に表示されます。

   ダウンロードされたパッケージは<サーバインストールフォルダ>¥PCCSRV¥Download¥Product に保存されます。

   注意

   プラグインマネージャでファイルがダウンロードできない場合は、24 時間後に自動的にダウンロードが再度行われます。プラグインマネージャを手動で起動してパッケージをダウンロードするには、Microsoft 管理コンソールから Apex One プラグインマネージャサービスを再起動します。
3. ダウンロードの進行状況を監視します。ダウンロード中に画面を切り替えることができます。

   パッケージのダウンロード中に問題が発生した場合は、Apex One 製品コンソールでサーバアップデートログを確認します。メインメニューで、[ログ] > [サーバアップデート] の順にクリックします。

   プラグインマネージャによってファイルがダウンロードされると、Trend Micro VDI オプションが新しい画面に表示されます。

   注意

   Trend Micro VDI オプションが表示されない場合は、766 ページの「プラグインマネージャのトラブルシューティング」を確認してください。
4. Trend Micro VDI オプションを今すぐインストールするには、[インストール] をクリックします。後でインストールするには

   a. [後でインストール] をクリックします。

b. [プラグインマネージャ] 画面を開きます。

c. [Trend Micro VDI オプション] セクションに移動し、[インストール] をクリックします。

5. 使用許諾契約書を読み、その条項に同意できる場合は [同意する] をクリックしてその条項に同意すると、

   インストールが開始されます。

6. インストールの進捗状況を監視します。インストールが完了すると、Trend Micro VDI オプションのバージョンが表示されます。

Trend Micro VDI オプションのライセンス

Trend Micro VDI オプションのライセンス情報の表示、アクティベート、およびサポート契約の更新には、プラグインマネージャを使用します。

トレンドマイクロからアクティベーションコードを入手し、このコードを使用して Trend Micro VDI オプションのすべての機能を有効化します。

Trend Micro VDI オプションのアクティベートまたはライセンス情報の更新

手順

1. Apex One Web コンソールを開いて、メインメニューで [プラグイン] をクリックします。
2. [プラグインマネージャ] 画面で、[Trend Micro VDI オプション] セクションに移動し、[プログラムの管理] をクリックします。
3. [ライセンス情報の表示] をクリックします。
4. [Trend Micro VDI オプションライセンスの詳細] 画面で、[製品ライセンスの新しいアクティベーションコード] をクリックします。
5. 表示された画面で、アクティベーションコードを入力して、[保存] をクリックします。

6. [Trend Micro VDI オプションライセンスの詳細] 画面に戻ったら、[ステータスをオンラインで確認] をクリックして、新しいライセンスの詳細と機能の状態で画面を更新します。この画面には、トレンドマイクロの Web サイトへのリンクも表示されます。このリンクに進むと、ライセンスに関する詳細情報を表示できます。

Trend Micro VDI オプションのライセンス情報の表示

手順

1. Apex One Web コンソールを開いて、メインメニューで [プラグイン] > (Trend Micro VDI オプション) [プログラムの管理] をクリックします。
2. [ライセンス情報の表示] をクリックします。
3. 開いた画面でライセンスの詳細を確認します。

   [Trend Micro VDI オプションライセンスの詳細] セクションに次の情報が表示されます。

   - ステータス: [アクティベーション完了]、[アクティベーション未完了]、または [サポート契約終了] が表示されます。
   - バージョン:[製品版] または [体験版] バージョンのいずれかが表示されます。製品版と体験版の両方がある場合は、表示されるバージョンは「製品版」です。
   - ライセンス有効期限:Trend Micro VDI オプションに複数のサポート契約がある場合、最も遅い日付の有効期限が表示されます。たとえば、ライセンスの有効期限が 2010 年 12 月 31 日と 2010 年 6 月 30 日の場合は、2010 年 12 月 31 日が表示されます。
   - アクティベーションコード:アクティベーションコードが表示されます。

   次の場合、ライセンスに関するメッセージが表示されます。

   製品版ライセンスを使用しているとき

   - 機能のサポート契約更新猶予期間である場合。更新猶予期間については、トレンドマイクロの販売代理店にお問い合わせください。

- サポート契約の有効期限が切れ、サポート契約更新猶予期間が経過した場合。この間、テクニカルサポートを受けることはできません。

体験版ライセンスを使用しているとき

- 体験版ライセンスの有効期限が切れた場合。この間、テクニカルサポートを受けることはできません。

4. ライセンスに関する情報を確認するには、トレンドマイクロ Web サイトで [詳細情報をオンラインで確認] をクリックします。
5. 画面を最新のライセンス情報に更新するには、[ステータスをオンラインで確認] をクリックします。

仮想サーバ接続

VMware vCenter 4 (VMware View 4)、Citrix XenServer 5.5 (Citrix XenDesktop 4)、または Microsoft Hyper-V Server を追加すると、オンデマンドの検索やコンポーネントのアップデートを最適化できます。Apex One サーバは、指定した仮想サーバと通信して、同じ物理サーバ上に存在するセキュリティエージェントを特定します。

その他の VDI サーバの場合、Apex One サーバは、仮想ハイパーバイザをエミュレートすることで他のプラットフォーム上の仮想エージェントを管理します。Apex One ハイパーバイザは、サーバが受信した順序で仮想エージェントの要求を処理します。Apex One サーバは要求を一度に 1 つずつ処理し、残りの要求はキューに配置します。

サーバ接続の追加

手順

1. Apex One Web コンソールを開いて、メインメニューで [プラグイン] > (Trend Micro VDI オプション) [プログラムの管理] をクリックします。
2. [VMware vCenter Server]、[Citrix XenServer]、[Microsoft Hyper-V]、または [その他の仮想化アプリケーション] を選択します。

注意

[その他の仮想化アプリケーション] を選択した場合、それ以外の情報は不要です。Apex One サーバは、受信した順序で仮想エージェントの要求に応答します。

3. サーバへの接続を有効にします。
4. 以下を指定します。
   - VMware vCenter および Citrix XenServer サーバの場合:
     - vCenter サーバの IP アドレス
     - ポート
     - 接続プロトコル (HTTP または HTTPS)
     - ユーザ名
     - パスワード
   - Microsoft Hyper-V サーバの場合:
     - Hyper-V プラットフォームのホスト名/IP アドレス
     - ドメイン\ユーザ名

       注意

       ログオンアカウントは、Administrators グループのドメインアカウントである必要があります。

     - パスワード
5. 必要に応じて、VMware vCenter または Citrix XenServer のプロキシ接続を有効にします。
   a. プロキシサーバの名前または IP アドレス、およびポートを指定します。
   b. プロキシサーバで認証が必要な場合は、ユーザ名とパスワードを指定します。

6. [接続テスト] をクリックして、Apex One サーバがこのサーバに正常に接続できることを確認します。

注意

Microsoft Hyper-V の接続に関するトラブルシューティングについては、721 ページの「Microsoft Hyper-V の接続に関するトラブルシューティング」を参照してください。

7. [保存] をクリックします。

他のサーバ接続の追加

手順

1. Apex One Web コンソールを開いて、メインメニューで [プラグイン] > (Trend Micro VDI オプション) [プログラムの管理] をクリックします。
2. [新しい vCenter 接続の追加]、[新しい XenServer 接続の追加]、または [新しい Hyper-V 接続の追加] をクリックします。
3. 上記の手順を繰り返して、適切なサーバ情報を入力します。
4. [保存] をクリックします。

接続設定の削除

手順

1. Apex One Web コンソールを開いて、メインメニューで [プラグイン] > (Trend Micro VDI オプション) [プログラムの管理] に移動します。
2. [この接続を削除] をクリックします。
3. [OK] をクリックして設定を削除します。
4. [保存] をクリックします。

VDI 検索能力の変更

管理者は、vdi.ini ファイルを変更することにより、同時に検索を実行する VDI エンドポイントの数を増やすことができます。システムリソースが増加した検索を確実に処理できるように、VDI の能力変更による影響を厳しく監視することをお勧めします。

手順

1. Apex One サーバコンピュータで、<サーバインストールフォルダ>PCCSRV¥Private¥vdi.ini に移動します。
2. [TaskController] 設定を探します。

   TaskController の初期設定は次のとおりです。

   - [TaskController]

     Controller_02_MaxConcurrentGuests=1

     Controller_03_MaxConcurrentGuests=3

     説明:

     - Controller_02_MaxConcurrentGuests=1 は、検索を同時に実行できるクライアントの最大数を示します。
     - Controller_03_MaxConcurrentGuests=3 は、アップデートを同時に実行できるクライアントの最大数を示します。
3. 必要に応じて各コントローラのカウントを増加または減少します。

   すべての設定について最小値は 1 です。

   すべての設定について最大値は 65536 です。
4. vdi.ini ファイルを保存して閉じます。
5. Apex One Master Service を再起動します。
6. VDI エンドポイントの CPU、メモリ、ディスク使用リソースを監視します。1 から 5 の手順を繰り返し、コントローラの設定をさらに変更して、

VDI 環境に最適になるように、同時に実行する検索の数を増加/減少します。

Microsoft Hyper-V の接続に関するトラブルシューティング

Microsoft Hyper-V の接続では、エージェントとサーバ間の通信に Windows Management Instrumentation (WMI) および DCOM が使用されます。ファイアウォールポリシーにより、この通信がブロックされて Hyper-V サーバに接続できないことがあります。

Hyper-V サーバの初期設定の待機ポートはポート 135 であり、以降の通信にはランダムに設定されたポートが選択されます。ファイアウォールが WMI トラフィックまたはこれら 2 つのポートのいずれかをブロックした場合、サーバとの通信は失敗します。管理者はファイアウォールポリシーを変更して、Hyper-V サーバとの通信を確立することができます。

IP アドレス、ドメイン\ユーザ名、パスワードを含むすべての設定が正しいことを確認してから、次のファイアウォールの変更を実施してください。

Windows ファイアウォールによる WMI 通信の許可

手順

1. Hyper-V サーバで、Windows ファイアウォールの [許可されたプログラム] 画面を開きます。

   Windows 2008 R2 システムで、[コントロール パネル] > [システムとセキュリティ] > [Windows ファイアウォール] > [Windows ファイアウォールによるプログラムの許可] に移動します。

2. [Windows Management Instrumentation (WMI)] を選択します。
3. [保存]をクリックします。
4. Hyper-V の接続を再度テストします。

Windows ファイアウォールまたはサードパーティファイアウォールを使用する場合の通信ポート

手順

1. Hyper-V サーバでは、ファイアウォールでポート 135 による通信が許可されることを確認し、Hyper-V の接続を再度テストしてください。

   ポートの詳細については、ファイアウォールのマニュアルを参照してください。

2. Hyper-V サーバとの接続が失敗した場合は、WMI を設定して固定ポートを使用します。

   WMI の固定ポートの設定の詳細については、次を参照してください。

   https://docs.microsoft.com/en-us/windows/desktop/WmiSdk/setting-up-a-fixed-port-for-wmi

3. ファイアウォールを使用した通信では、ポート 135 および新しく作成した固定ポート (24158) のみを開きます。

4. Hyper-V の接続を再度テストします。

VDI 事前検索テンプレート生成ツール

オンデマンドの検索を最適化したり、ベースまたはゴールドイメージから GUID を削除するには、Apex One VDI 事前検索テンプレート生成ツールを使用します。このツールは、ベースまたはゴールドイメージを検索し、イメージを認定します。このイメージの複製を検索する際は、Apex One では変更された部分のみを確認します。これにより、検索時間が短縮されます。

ヒント

Windows Update の適用後、または新しいアプリケーションのインストール後に、事前検索テンプレートを生成することをお勧めします。

ツールを使用した事前検索テンプレートの作成

手順

1. Apex One サーバコンピュータで、<サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility¥TCacheGen に移動します。
2. VDI 事前検索テンプレート生成ツールのバージョンを選択します。次のバージョンを使用できます。

   表 15-14. VDI 事前検索テンプレート生成ツールのバージョン

ファイル名	手順
TCacheGen.exe	32 ビットプラットフォーム上でツールを直接実行する場合は、このファイルを選択します。
TCacheGen_x64.exe	64 ビットプラットフォーム上でツールを直接実行する場合は、このファイルを選択します。

3. 対象の VM テンプレート上の任意のディレクトリにツールをコピーします。

   重要

   TCacheGen.exe は、ネットワーク共有を介して実行することはできません。ローカルの VM テンプレートにコピーする必要があります。VM テンプレートのアーキテクチャ (64 ビットまたは 32 ビット) に応じて、適切なツールをコピーするようにしてください。

4. TCacheGen.exe または TCacheGen_x64.exe をダブルクリックします。
5. [事前検索テンプレートを生成して GUID を削除する] を選択し、[次へ] をクリックします。
6. セキュリティエージェントのアンロードパスワードを指定します (該当する場合)。

   事前検索テンプレートを生成して GUID を削除する前に、ツールはイメージにセキュリティ上の脅威がないかどうか検索します。

事前検索テンプレートの生成後、ツールは自動的にセキュリティエージェントをアンロードし、TCacheGen.exe または TCacheGen_x64.exe プログラムを削除します。

セキュリティエージェントはリロードしないでください。セキュリティエージェントがリロードされた場合は、事前検索テンプレートを再度作成する必要があります。

CLI を使用した事前検索テンプレートの作成

手順

1. Apex One サーバコンピュータで、<サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility¥TCacheGen に移動します。
2. VDI 事前検索テンプレート生成ツールのバージョンを選択します。次のバージョンを使用できます。

   表 15-15. VDI 事前検索テンプレート生成ツールのバージョン

ファイル名	手順
TCacheGen.exe TCacheGenCli.exe	32 ビットプラットフォームのコマンドラインインタフェースからツールを実行する場合は、TCacheGenCli.exe ファイルと TCacheGen.exe の両方を選択します。
TCacheGen_x64.exe TCacheGenCli_x64.exe	64 ビットプラットフォームのコマンドラインインタフェースからツールを実行する場合は、TCacheGenCli_x64.exe と TCacheGen_x64.exe の両方を選択します。

3. 対象の VM テンプレートのセキュリティエージェントをアンロードします。
4. 前の手順で選択したツールのバージョンを、対象の VM テンプレート内の<エージェントのインストールフォルダ>にコピーします。

重要

TCacheGen.exe は、ネットワーク共有を介して実行することはできません。ローカルの VM テンプレートにコピーする必要があります。VM テンプレートのアーキテクチャ (64 ビットまたは 32 ビット) に応じて、適切なツールをコピーするようにしてください。

5. 事前検索を実行できるようにセキュリティエージェントプログラムを再起動します。
6. コマンドプロンプトを開いて、ディレクトリを<エージェントのインストールフォルダ>に変更します。
7. 次のいずれかのコマンドを使用して、ツールを実行します。
   - 32 ビット版システムの場合: `TCacheGenCli Generate_Template`
   - 64 ビット版システムの場合: `TcacheGenCli_x64 Generate_Template`

注意

事前検索テンプレートを生成して GUID を削除する前に、ツールはイメージにセキュリティ上の脅威がないかどうか検索します。

事前検索テンプレートの生成後、ツールは自動的にセキュリティエージェントをアンロードし、`TCacheGen.exe` または `TCacheGen_x64.exe` プログラムを削除します。必要に応じて、関連付けられている `TCacheGenCli.exe` または `TCacheGenCli_x64.exe` を手動で削除する必要があります。

セキュリティエージェントはリロードしないでください。セキュリティエージェントがリロードされた場合は、事前検索テンプレートを再度作成する必要があります。

テンプレートからの GUID の削除

手順

1. Apex One サーバコンピュータで、<サーバインストールフォルダ>`¥PCCSRV¥Admin¥Utility¥TCacheGen` に移動します。

2. VDI 事前検索テンプレート生成ツールのバージョンを選択します。次のバージョンを使用できます。

   表 15-16. VDI 事前検索テンプレート生成ツールのバージョン

ファイル名	手順
TCacheGen.exe	32 ビットプラットフォーム上でツールを直接実行する場合は、このファイルを選択します。
TCacheGen_x64.exe	64 ビットプラットフォーム上でツールを直接実行する場合は、このファイルを選択します。
TCacheGenCli.exe	32 ビットプラットフォームのコマンドラインインタフェースからツールを実行する場合は、`TCacheGenCli.exe` ファイルと `TCacheGen.exe` の両方を選択します。
TCacheGenCli_x64.exe	64 ビットプラットフォームのコマンドラインインタフェースからツールを実行する場合は、`TCacheGenCli_x64.exe` と `TCacheGen_x64.exe` の両方を選択します。

3. 前の手順で選択したツールのバージョンを、対象の VM テンプレート内の<エージェントのインストールフォルダ>にコピーします。

4. ツールを実行します。

   - ツールを直接実行するには

     a. `TCacheGen.exe` または `TCacheGen_x64.exe` をダブルクリックします。

     b. [事前検索テンプレートから GUID を削除する] を選択し、[次へ] をクリックします。

   - ツールをコマンドラインインタフェースから実行するには

     a. コマンドプロンプトを開いて、ディレクトリを<エージェントインストールフォルダ>に変更します。

     b. 次のコマンドを入力します。

     ```
     TCacheGenCli Remove GUID
     ```

     または

```
TcacheGenCli_x64 Remove GUID
```

グローバルエージェント設定

Apex One では、グローバルエージェント設定を、すべてのエージェントまたは特定の権限を持つエージェントにのみ適用します。

手順

1. [エージェント] > [グローバルエージェント設定] に移動します。
2. 次の設定を行います。

表 15-17. グローバルエージェント設定

タブ	設定	参照
セキュリティ設定	検索設定	343 ページの「検索設定セクション」
	予約検索設定	349 ページの「予約検索設定セクション」
	ファイアウォール設定	560 ページの「グローバルファイアウォール設定」
	不審接続監視設定	396 ページの「ユーザ指定の IP リストのグローバル設定」
	挙動監視設定	423 ページの「グローバル挙動監視設定」

タブ	設定	参照
システム	ソフトウェア安全性評価サービスの設定	341 ページの「グローバル検索設定」
	Smart Protection サービスプロキシ	691 ページの「グローバル Smart Protection サービスプロキシ設定」
	アップデート	• 241 ページの「セキュリティエージェントのアップデート元としてのアップデートサーバ」 • 253 ページの「セキュリティエージェントアップデートのディスク空き容量の設定」
	サービスの再起動	652 ページの「セキュリティエージェントサービスの再起動」
ネットワーク	優先 IP アドレス	142 ページの「エージェント IP アドレス」
	サーバ/エージェント間通信	630 ページの「サーバ/エージェント間通信の暗号化の強化」
	ウイルス/不正プログラムログ帯域幅設定	341 ページの「グローバル検索設定」
	到達不能ネットワーク	682 ページの「到達不能エージェント」
エージェント制御	一般設定	341 ページの「グローバル検索設定」
	警告設定	255 ページの「セキュリティエージェントのアップデート通知の設定」
	エージェント言語設定	659 ページの「セキュリティエージェント言語設定」

3. [保存] をクリックします。

エージェントの権限とその他の設定

セキュリティエージェントで特定の設定を変更したり高度なタスクを実行する権限をユーザに付与します。

注意

ウイルス対策設定は、Apex One ウイルス対策機能をアクティベートした後にのみ表示されます。

ヒント

組織全体で一貫した設定およびポリシーを実行するには、ユーザに権限を限定して付与します。

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを含めるか、特定のドメインまたはエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックします。
4. [権限] タブで次のユーザの権限を設定します。

表 15-18. エージェント権限

エージェント権限	レファレンス/参照情報
スタンドアロンモード権限	656 ページの「セキュリティエージェントのスタンドアロンモード権限」
検索権限	329 ページの「検索の種類権限」
予約検索権限	330 ページの「予約検索権限とその他の設定」
ファイアウォール権限	558 ページの「ファイアウォール権限」
挙動監視権限	424 ページの「挙動監視権限」

エージェント権限	レファレンス/参照情報
信頼済みプログラムリスト	340 ページの「信頼済みプログラムリスト権限」
メール検索権限	334 ページの「メール検索権限とその他の設定」
プロキシ設定権限	692 ページの「プロキシ設定権限の付与」
コンポーネントのアップデート	251 ページの「アップデート権限とその他の設定」
アンロードとロック解除	655 ページの「エージェントのアンロードとロック解除権限の付与」
アンインストール	201 ページの「セキュリティエージェントのアンインストール権限の付与」

5. [その他の設定] タブをクリックして、次の設定を行います。

表 15-19. その他のエージェント設定

設定	レファレンス/参照情報
アップデート設定	251 ページの「アップデート権限とその他の設定」
Web レピュテーション設定	524 ページの「エージェントユーザ向けの Web からの脅威の通知」
挙動監視設定	424 ページの「挙動監視権限」
C&C コンタクトアラート設定	529 ページの「エージェントユーザ向けの C&C コンタクトアラート通知」
隔離の一括復元通知設定	隔離ファイルの復元後にエンドポイントに通知メッセージを表示します。
機械学習型検索設定	不明な脅威の検出後にエンドポイントに通知メッセージを表示します。
予約検索設定	332 ページの「予約検索権限の付与と権限の通知の表示」
検索用のキャッシュ設定	336 ページの「検索用のキャッシュ設定」

設定	レファレンス/参照情報
POP3 メール検索設定	335 ページの「メール検索権限の付与と POP3 メール検索の有効化」
セキュリティエージェントアクセス制限	653 ページの「セキュリティエージェントコンソールアクセス制限」
再起動の通知	358 ページの「セキュリティエージェントユーザ向けのセキュリティリスクの通知」

6. エージェントツリーでドメインまたはエージェントを選択した場合は、[保存] をクリックします。ルートドメインアイコンをクリックした場合は、次のオプションのいずれかを選択します。

   - すべてのエージェントに適用: すべての既存のエージェント、および既存または今後追加されるドメインに加えられる新しいエージェントに、設定を適用します。今後追加されるドメインとは、設定を指定した時点でまだ作成されていないドメインのことです。
   - 今後追加されるドメインにのみ適用: 今後追加されるドメインに加えられるエージェントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいエージェントには設定を適用しません。

パート IV

保護の強化

第 16 章

オフプレミスエージェントの保護

この章では、組織のイントラネット外のセキュリティエージェントを保護するために必要なエッジリレーサーバのインストールと設定の手順について説明します。

この章は次のトピックで構成されます。

エッジリレーサーバ

Apex One エッジリレーサーバを使用すると、ユーザが組織のイントラネット外に持ち出したエンドポイントについても、その状況を監視し、保護を強化することができます。エッジリレーサーバを非武装地帯 (DMZ) にインストールすることで、Apex One サーバへの接続を直接確立できないオフプレミスのセキュリティエージェントでも、サーバをポーリングして更新されたポリシー設定を受け取ることができます。

エッジリレーサーバの設定が完了すると、その設定がセキュリティエージェントに配信され、Apex One サーバへの接続が利用できない場合に自動的にエッジリレーサーバに接続されるようになります。

エッジリレーサーバ、Apex One サーバ、およびセキュリティエージェントの間の通信は、証明書認証を使用して暗号化されます。

詳細については、752 ページの「エッジリレーサーバの証明書の管理」を参照してください。

エッジリレーサーバのシステム要件

システム要件の完全なリストについては、次の Web サイトを参照してください。

http://www.go-tm.jp/corp/req

エッジリレーサーバのインストール

エッジリレーサーバをインストールする前に、対象のサーバコンピュータがシステムの最小要件を満たしていることを確認してください。

詳細については、736 ページの「エッジリレーサーバのシステム要件」を参照してください。

手順

1. Apex One サーバコンピュータの <サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility¥EdgeServer フォルダを選択し、対象のエッジリレーサーバコンピュータにフォルダをコピーします。
2. 対象のエッジリレーサーバで、EdgeServer フォルダを開き、setup.exe ファイルを実行してインストールプロセスを開始します。

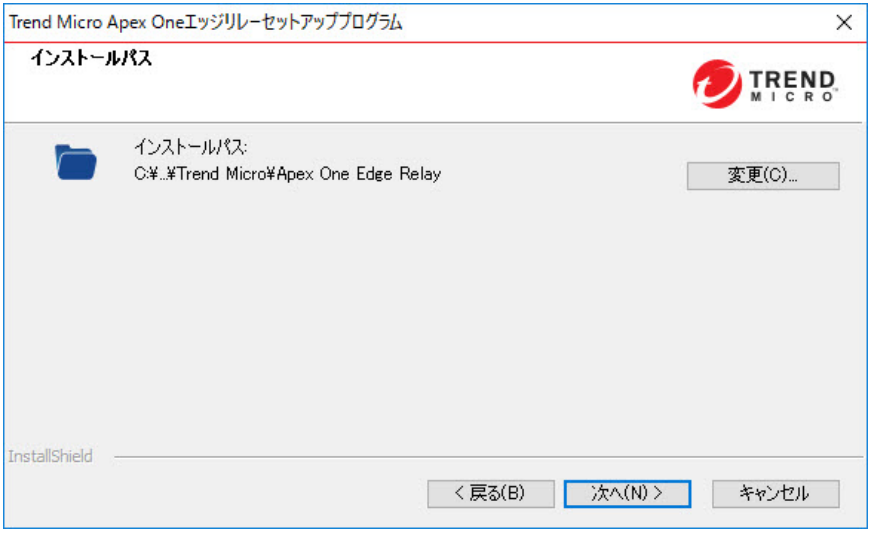
   サーバに必要なコンポーネントが揃っているかがチェックされます。
3. サーバに次のコンポーネントがない場合は、[インストール] をクリックし、エッジリレーサーバのインストール時にインストールされるようにします。

   - Microsoft Visual C++ 2017 Update 3 再頒布可能パッケージ (x86)
   - Microsoft Visual C++ 2017 Update 3 再頒布可能パッケージ (x64)
   - Microsoft .NET Framework 4.6.1
   - Microsoft URL Rewrite Module 2.0 for IIS (x64)
   - Microsoft Application Request Routing 3.0 (x64)

   [ようこそ] 画面が表示されます。
4. [次へ] をクリックします。

[インストールパス] 画面が表示されます。

5. 初期設定のインストールディレクトリをそのまま使用するか、[変更] をクリックして別の場所を選択します。



6. [次へ] をクリックします。

   [エッジリレーサーバとセキュリティエージェントの接続] 画面が表示されます。

7. オフプレミスのセキュリティエージェントからエッジリレーサーバへの接続に使用する次の設定を指定します。

   - エッジリレーサーバの FQDN: エッジリレーサーバの FQDN を入力します。
   - 証明書: エッジリレーサーバの Web ホスト証明書を選択します。選択せずに [次へ] をクリックすると、自己署名証明書が作成されます。

   注意

   ただちに使用できるカスタム証明書がない場合は、インストールの完了後に、エッジリレーサーバ登録ツールを使用して自己署名証明書を変更できます。

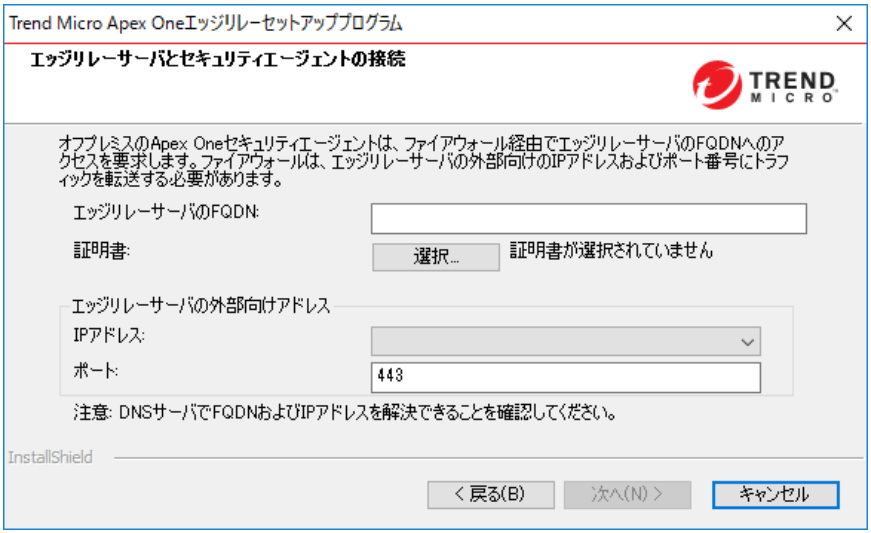
   詳細については、750 ページの「エッジリレーサーバとユーザ独自の証明書のバインド」を参照してください。

- IP アドレス: サーバの IP アドレスを選択します。
- ポート: 初期設定のポートをそのまま使用するか別のポートを指定します。

重要

ファイアウォールおよびゲートウェイの設定で以下を許可する必要があります。

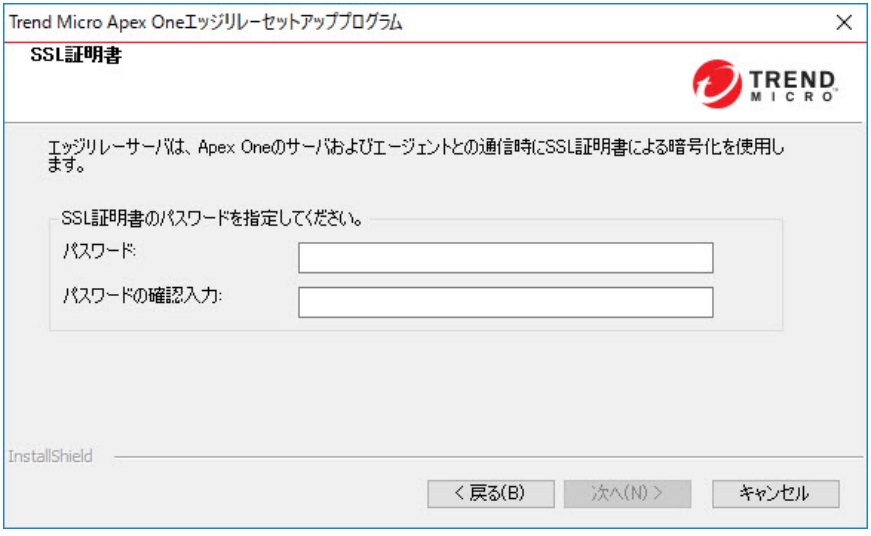
- インターネットからエッジリレーサーバへのセキュリティエージェント通信のリダイレクト
- 指定したポート経由の通信



8. [次へ] をクリックします。

   [SSL 証明書] 画面が表示されます。

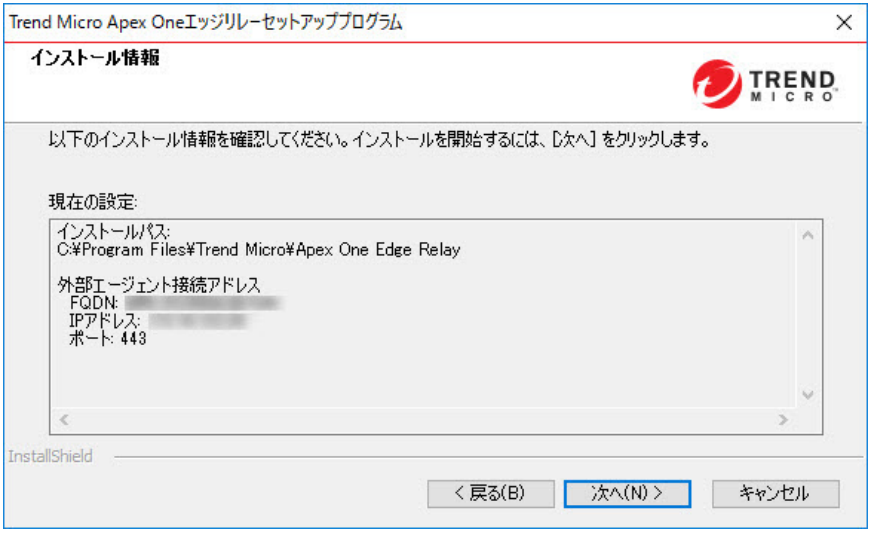
9. エッジリレーサーバの証明書 (OsceOPA 証明書) に使用するパスワードを入力し、確認のためにもう一度入力します。



10. [次へ] をクリックします。

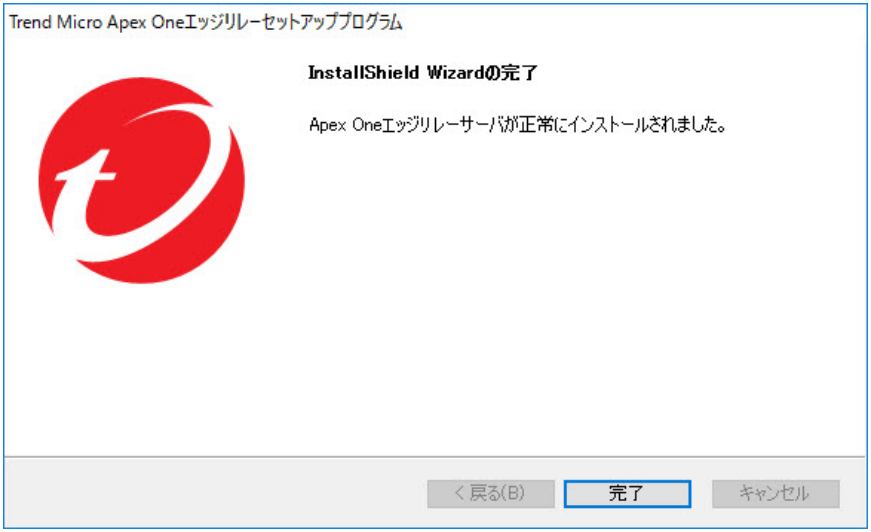
    [インストール情報] 画面が表示されます。

11. [次へ >] をクリックしてインストールを開始します。



インストールが完了すると、[InstallShield Wizard の完了] 画面が表示されます。

12. [完了] をクリックします。



エッジリレーサーバを使用する準備はこれで完了です。どの Apex One サーバをエッジリレーサーバでサポートするかを設定できます。

詳細については、745 ページの「エッジリレーサーバ登録ツール」を参照してください。

注意

- Apex One が使用するポートとプロトコルを許可するようにファイアウォールまたはセキュリティルータを設定します。ポートとプロトコルのリストについては、https://success.trendmicro.com/jp/solution/1123355 を参照してください。
- エッジリレーサーバでの DNS 名前解決をチェックします。セキュリティエージェントで使用する Apex One サーバのホスト名と FQDN がエッジリレーサーバで解決可能であることを確認してください。

エッジリレーサーバのバージョンアップ

Apex One エッジリレーサーバは、旧バージョンのエッジリレーサーバからのバージョンアップをサポートしています。バージョンアッププロセスを実行

すると、旧バージョンで使用されていたサーバ設定がセットアッププログラムによって自動的に適用され、すべての証明書が転送されます。

重要

このバージョンのエッジリレーサーバは、古いバージョンのエージェントプログラムをサポートしていません。オフプレミスのエンドポイントを管理する必要がある場合は、すべてのエージェントを Apex One セキュリティエージェントにバージョンアップし、セキュリティエージェントを Apex One サーバに接続してバージョンアップ後のエッジリレー設定を取得する必要があります。

エッジリレーサーバをバージョンアップする前に、対象のサーバコンピュータがシステムの最小要件を満たしていることを確認してください。

詳細については、736 ページの「エッジリレーサーバのシステム要件」を参照してください。

手順

1. Apex One サーバコンピュータの <サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility¥EdgeServer フォルダを選択し、対象のエッジリレーサーバコンピュータにフォルダをコピーします。
2. 対象のエッジリレーサーバで、EdgeServer フォルダを開き、setup.exe ファイルを実行してバージョンアッププロセスを開始します。

   [ようこそ] 画面が表示されます。
3. [次へ>] をクリックします。

   セットアッププログラムにより以前のエッジリレーサーバから必要な設定が自動的に取得され、[インストール情報] 画面が表示されます。
4. [次へ >] をクリックしてバージョンアップを開始します。
5. バージョンアップの完了後、エッジリレーサーバ登録ツールを使用してバージョンアップ後のエッジリレーサーバを Apex One サーバに登録する必要があります。

   a. エッジリレーサーバ登録ツールを探します。エッジリレーサーバコンピュータの次の場所にあります。

<Apex One エッジリレーのインストールディレクトリ>¥OfcEdgeSvc¥ofcedgecfg.exe

b. 管理者権限を使用してコマンドラインエディタを開きます。

cmd.exe を右クリックして、[管理者として実行] をクリックします。

c. ディレクトリを ofcedgecfg.exe ファイルの場所に切り替えます。

d. 次のコマンドを実行します。

ofcedgecfg.exe --cmd reg --server <Apex One サーバのアドレス> --port <Apex One サーバのポート> --pwd <Apex One の root アカウントのパスワード>

Apex One Web コンソールでバージョンアップ後のエッジリレーサーバの登録が正常に完了したことを確認します ([管理] > [設定] > [エッジリレー])。

6. エッジリレーサーバを使用して管理するすべてのセキュリティエージェントが Apex One サーバに直接接続して最新のエッジリレーサーバ設定を取得できることを確認します。

エッジリレーサーバ登録ツール

エッジリレーサーバをインストールしたら、エッジリレーサーバ登録ツールを使用してエッジリレーサーバをオフプレミスのセキュリティエージェントがレポートする Apex One サーバに登録する必要があります。Apex One サーバにレポートするセキュリティエージェントは登録された接続設定を受け取り、社内イントラネット外でもエッジリレーサーバを使用して Apex One サーバをポーリングできるようになります。

エッジリレーサーバ登録ツールでは、コマンドラインエディタを使用して次のタスクを実行できます。

- 747 ページの「Apex One サーバへの登録」
- 747 ページの「Apex One サーバからの登録の解除」
- 748 ページの「自己署名証明書の更新 (OsceEdgeRoot CA、webhost、OsceOPA を含む)」

- 749 ページの「Webhost 証明書および OsceOPA 証明書との独自の証明書のバインド」
- 750 ページの「すべての IIS ルールの削除 (すべての Apex One サーバから登録を解除した後)」

エッジリレーサーバ登録ツールの使用

エッジリレーサーバ登録ツールでは、コマンドラインエディタを使用して次のタスクを実行できます。

- 747 ページの「Apex One サーバへの登録」
- 747 ページの「Apex One サーバからの登録の解除」
- 748 ページの「自己署名証明書の更新 (OsceEdgeRoot CA、webhost、OsceOPA を含む)」
- 749 ページの「Webhost 証明書および OsceOPA 証明書との独自の証明書のバインド」
- 750 ページの「すべての IIS ルールの削除 (すべての Apex One サーバから登録を解除した後)」

注意

エッジリレーサーバは複数の Apex One サーバに登録できます。必要な Apex One 接続のそれぞれについて登録コマンドを個別に実行します。

手順

1. エッジリレーサーバ登録ツールを探します。エッジリレーサーバコンピュータの次の場所にあります。

   `<Apex One エッジリレーのインストールディレクトリ>¥OfcEdgeSvc¥ofcedgecfg.exe`

2. 管理者権限を使用してコマンドラインエディタを開きます。

   `cmd.exe` を右クリックして、[管理者として実行] をクリックします。

3. ディレクトリを ofcedgecfg.exe ファイルの場所に切り替えます。
4. 必要なタスクを実行します。

Apex One サーバへの登録

コマンド	--cmd reg	
パラメータ	--server <値>	Apex One サーバの IP アドレス
	--port <値>	Apex One サーバのポート番号
	--pwd <値>	Apex One サーバの「ルート」アカウントのパスワード
例	ofcedgecfg.exe --cmd reg --server <サーバアドレス> --port <ポート> --pwd <ルートのパスワード>	

Apex One サーバからの登録の解除

コマンド	--cmd unreg	
パラメータ	--server <値>	Apex One サーバの IP アドレス
	--port <値>	Apex One サーバのポート番号
	--pwd <値>	Apex One サーバの「ルート」アカウントのパスワード
例	ofcedgecfg.exe --cmd unreg --server <サーバアドレス> --port <ポート> --pwd <ルートのパスワード>	

自己署名証明書の更新 (OsceEdgeRoot CA、webhost、OsceOPA を含む)

警告!

エッジリレーセットアッププログラムで作成した証明書を使用する場合は、必ず `renewcert` コマンドを使用してください。ユーザ独自の証明書を使用するエッジリレーサーバで `renewcert` を実行すると、ユーザ独自の証明書が削除され、自己署名証明書に置き換わります。

コマンド	`--cmd renewcert`	
パラメータ	`--opacertpwd <値>`	OsceOPA 証明書のパスワード
	`--keeprootca`	証明書の更新後にルート CA を保持 (オプション)
例	`ofcedgecfg.exe --cmd renewcert --opacertpwd <OsceOPA 証明書のパスワード> [--keeprootca]`	
次に必要なコマンド	証明書を更新した後に、エッジリレーサーバを Apex One サーバに再登録する必要があります。 詳細については、747 ページの「Apex One サーバへの登録」を参照してください。 **重要** Apex One サーバに再登録した後は、すべてのオフプレミスのセキュリティエージェントが Apex One サーバに再接続して、更新後の証明書を取得する必要があります。最新の証明書を受け取っていないオフプレミスのセキュリティエージェントは、エッジリレーサーバに接続できません。	

Webhost 証明書および OsceOPA 証明書との独自の証明書のバインド

重要

ユーザ独自の証明書をエッジリレーサーバにバインドするには、Webhost 証明書および OsceOPA 証明書を準備し、正しく構成する必要があります。

ユーザ独自の証明書の準備とバインドを実行する方法の詳細については、750 ページの「エッジリレーサーバとユーザ独自の証明書のバインド」を参照してください。

コマンド	`--cmd bindwebsite`	
パラメータ	`--certsubject <値>`	Webhost 証明書の件名
	`--certstore <値>`	Webhost 証明書のストア名: `My | webhosting`
	`--certissuer <値>`	Webhost 証明書の発行元
	`--opacertpwd <値>`	OsceOPA 証明書のパスワード
例	`ofcedgecfg.exe --cmd bindwebsite --certsubject <証明書の件名> --certstore <証明書ストア名> --certissuer <証明書の発行元> --opacertpwd <OsceOPA 証明書のパスワード>`	
次に必要なコマンド	ユーザ独自の証明書をバインドした後は、エッジリレーサーバを Apex One サーバに再登録する必要があります。 詳細については、747 ページの「Apex One サーバへの登録」を参照してください。 **重要** Apex One サーバに再登録した後は、すべてのオフプレミスのセキュリティエージェントが Apex One サーバに再接続して、更新後の証明書を取得する必要があります。最新の証明書を受け取っていないオフプレミスのセキュリティエージェントは、エッジリレーサーバに接続できません。	

すべての IIS ルールの削除 (すべての Apex One サーバから登録を解除した後)

コマンド	`--cmd delrule`
パラメータ	なし
例	`ofcedgecfg.exe --cmd delrule`

エッジリレーサーバとユーザ独自の証明書のバインド

ユーザ独自の証明書の作成とバインドを実行して、Apex One サーバおよびセキュリティエージェントとエッジリレーサーバとの間の通信を検証できます。

重要

ユーザ独自の証明書を使用する場合は、その証明書に公開鍵と秘密鍵の両方を含めて、他の証明書をサインアウトする必要があります。

公開鍵と秘密鍵の要件により、大部分のサードパーティの商用 CA を利用できない可能性があります。

手順

1. カスタム Webhost 証明書を準備します。
   - 信頼されたストアに含まれる CA によって発行された証明書を使用する必要があります。
   - 保存先は「Web ホスティング」証明書ストア (「My」または「webhosting」) とします。
   - バインド時に必要な以下の情報を記録しておきます。
     - 証明書の件名
     - 証明書の発行元

重要

ユーザ独自の証明書を使用する場合は、その証明書に公開鍵と秘密鍵の両方を含めて、他の証明書をサインアウトする必要があります。

公開鍵と秘密鍵の要件により、大部分のサードパーティの商用 CA を利用できない可能性があります。

2. 自己署名証明書である OsceOPA 証明書に代わる有効な証明書を準備します。

   - 信頼されたストアに含まれる CA によって発行された証明書を使用する必要があります。
   - 証明書の件名は `OsceOPA` とします。

     重要

     証明書の件名では大文字と小文字が区別されます。

   - 保存先は「OfcEdge」証明書ストアとし、そのストアから他の証明書を削除します。

3. エッジリレーサーバ登録ツールを探します。エッジリレーサーバコンピュータの次の場所にあります。

   `<Apex One エッジリレーのインストールディレクトリ>¥OfcEdgeSvc¥ofcedgecfg.exe`

4. 管理者権限を使用してコマンドラインエディタを開きます。

   `cmd.exe` を右クリックして、[管理者として実行] をクリックします。

5. ディレクトリを `ofcedgecfg.exe` ファイルの場所に切り替えます。

6. 次のコマンドを実行します。

   `ofcedgecfg.exe --cmd bindwebsite --certsubject <Webhost 証明書の件名> --certstore <My | webhosting> --certissuer <Webhost 証明書の発行元> --opacertpwd <OsceOPA 証明書のパスワード>`

7. 次のコマンドを実行して、Apex One サーバにエッジリレーサーバを再登録します。

```
ofcedgecfg.exe --cmd reg --server <サーバアドレス> --port <ポート> --pwd <ルートのパスワード>
```

8. セキュリティエージェントが新しい証明書を受信し、エッジリレーサーバに再接続できるように、オフプレミスのユーザにローカルイントラネットに直接接続するよう指示します。

Apex One でのエッジリレーサーバ接続の確認

エッジリレーサーバへの接続後、Apex One サーバにレポートするセキュリティエージェントに接続設定が配信され、組織のイントラネット外では自動的にエッジリレーサーバと通信できるようになります。その後、[エッジリレー設定] 画面でエッジリレーサーバの接続状態を監視できます。

手順

1. Apex One Web コンソールで、[管理] > [設定] > [エッジリレー] に移動します。

   [エッジリレー設定] 画面が表示されます。

2. Apex One サーバに現在登録されているエッジリレーサーバを確認します。

エッジリレーサーバの証明書の管理

Apex One には、エージェントがエッジリレーサーバとの通信に使用する証明書を作成または更新するためのコマンドラインツールが用意されています。新しい証明書を作成すると、エッジリレーサーバから Apex One サーバに新しい証明書が送信され、エージェントが Apex One サーバに次回接続したときにサーバからエージェントに証明書が配信されます。

重要

オフプレミスのセキュリティエージェントは、Apex One サーバに接続してエッジリレーサーバの新しい証明書を取得する必要があります。アップデートされた証明書を取得していないオフプレミスエージェントは、Apex One サーバとの接続を確立するまではエッジリレーサーバと通信できなくなります。

手順

1. エッジリレーサーバで、コマンドラインエディタを開き、次のディレクトリに移動します。

   ```
   C:¥Program Files¥Trend Micro¥Apex One Edge Relay¥OfcEdgeSvc¥
   ```

2. 次のコマンドを入力して証明書ツールを実行します。

   ```
   ofcedgecfg.exe --cmd renewcert --opacertpwd <OsceOPA 証明書のパスワード> [--keeprootca]
   ```

   説明:

   - `--renewcert`:新しい証明書を作成します。
   - `--opacertpwd <パスワード>`: 証明書パッケージのパスワードを指定します。

   エッジリレーサーバで新しい証明書パッケージが作成され、自動的に Apex One サーバに送信されます。セキュリティエージェントから Apex One サーバへの次回のレポート時に、Apex One サーバからセキュリティエージェントに新しい証明書が配信されます。

第 17 章

プラグインマネージャの使用

ここでは、プラグインマネージャの設定方法と、プラグインマネージャを介して配信されるプラグインソリューションの概要について説明します。

この章は次のトピックで構成されます。

プラグインマネージャについて

Apex One には、既存の Apex One 環境に新しいソリューションを統合するプラグインマネージャというフレームワークが含まれています。これらのソリューションの管理を容易にするために、プラグインマネージャでは、ソリューションのデータがウィジェットに一覧表示されます。

注意

現時点では、いずれのプラグインソリューションも IPv6 をサポートしていません。サーバはこれらのソリューションをダウンロードできますが、IPv6 シングルスタックのセキュリティエージェントおよび IPv6 シングルスタックホストに配信することはできません。

プラグインマネージャは次の機能を提供します。

- 組み込みの Apex One 機能

  組み込みの Apex One 機能の中には、個別にライセンスされ、プラグインマネージャを通じてアクティベートされるものがあります。今回のリリースでは、「Trend Micro VDI オプション」と「Apex One 情報漏えい対策オプション」の 2 つの機能がこのカテゴリに分類されます。

- プラグインプログラム

  プラグインプログラムは、Apex One プログラムの一部ではありません。プラグインプログラムには個別のライセンスと管理コンソールがあります。管理コンソールには、Apex One Web コンソール内からアクセスします。プラグインプログラムの例として、Trend Micro Apex One ToolBox、Trend Micro Apex One (Mac) があります。

- ダッシュボードのタブとウィジェット

  Apex One の ダッシュボード 画面に Apex One サーバおよびエージェントの保護ステータスを監視するタブやウィジェットを表示するには、プラグインマネージャが必要です。

このドキュメントでは、プラグインプログラムのインストールと管理の全般的な概要とともに、ウィジェットで使用可能なプラグインプログラムのデー

タについて説明します。特定のプラグインプログラムの設定と管理の詳細については、プログラムのドキュメントを参照してください。

エンドポイント上のプラグインプログラムエージェント

Apex One (Mac) などの一部のプラグインプログラムでは、エンドポイントの Windows OS にエージェントがインストールされます。これらのエージェントは、CNTAoSMgr.exe というプロセス名で実行されるセキュリティエージェントプラグインマネージャで管理されます。

CNTAoSMgr.exe はセキュリティエージェントとともにインストールされます。CNTAoSMgr.exe の唯一の追加要件として、Microsoft XML Parser (MSXML) バージョン 3.0 以降が必要です。

注意

その他のプラグインプログラムのエージェントは Windows OS にインストールされないため、セキュリティエージェントプラグインマネージャでは管理されません。このようなエージェントの例として、Apex One (Mac) セキュリティエージェントがあります。

ウィジェット

ウィジェットには、導入したプラグインソリューションのデータが一覧表示されます。ウィジェットは、Apex One サーバの ダッシュボード 画面で使用できます。「Apex One とプラグインの統合管理」という特殊なウィジェットでは、セキュリティエージェントのデータとプラグインソリューションのデータが組み合わされ、それらのデータがエージェントツリーに表示されます。

この管理者ガイドでは、ウィジェットとウィジェットをサポートするソリューションの概要について説明します。

プラグインマネージャのインストール

以前のバージョンのプラグインマネージャでは、プラグインマネージャのインストールパッケージがトレンドマイクロのアップデートサーバからダウン

ロードされ、Apex One サーバをホストするコンピュータにインストールされます。このバージョンでは、プラグインマネージャのインストールパッケージが Apex One サーバのインストールパッケージの次の場所に含まれています。

<サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility¥PLM¥PLMSetup.exe

この PLMSetup.exe ファイルを実行すると、プラグインマネージャがインストールされます。

Apex One のインストールを完了すると、Apex One を新しくインストールしたユーザには、Apex One サーバとプラグインマネージャの両方がインストールされます。すでにプラグインマネージャを使用しているユーザがこのバージョンの Apex One にバージョンアップする場合は、プラグインマネージャサービスを停止してから、インストールパッケージを実行する必要があります。

インストール後のタスクの実行

プラグインマネージャをインストールした後、次のタスクを実行します。

手順

1. Apex One Web コンソールを開いて、メインメニューで [プラグイン] をクリックします。
2. プラグインソリューションを管理します。
3. Apex One Web コンソールの ダッシュボード 画面にアクセスして、プラグインソリューションのウィジェットを管理します。

組み込みの Apex One 機能の管理

組み込みの Apex One 機能は Apex One とともにインストールされ、管理者がプラグインマネージャから各機能をアクティベートします。Trend Micro VDI オプションのようにプラグインマネージャで管理する機能もあれば、情

報漏えい対策オプションのように Web コンソールで管理する機能もあります。

プラグインプログラムの管理

プラグインプログラムは Apex One とは別にインストールしてアクティベートします。各プラグインには、個別の管理コンソールが用意されています。これらの管理コンソールには、Web コンソールからアクセスできます。

プラグインプログラムのインストール

プラグインプログラムは、[プラグインマネージャ]コンソールに表示されます。コンソールで、プログラムをダウンロードしてインストールし、管理することができます。プラグインプログラムのインストールパッケージは、プラグインマネージャによってトレンドマイクロのアップデートサーバまたはユーザ指定のアップデート元 (正しく設定されている場合) からダウンロードされます。トレンドマイクロのアップデートサーバからパッケージをダウンロードするには、インターネット接続が必要です。

プラグインマネージャによってインストールパッケージがダウンロードされるか、インストールが開始されると、他のプラグインプログラムのダウンロード、インストール、バージョンアップなどの機能は一時的に使用できなくなります。

プラグインマネージャは、Apex Central のシングルサインオン機能によるプラグインプログラムのインストールおよび管理をサポートしていません。

プラグインプログラムのインストール

手順

1. Apex One Web コンソールを開いて、メインメニューで [プラグイン] をクリックします。
2. [プラグインマネージャ] 画面で、プラグインプログラムのセクションに移動し、[ダウンロード] をクリックします。

[ダウンロード] ボタンの横に、プラグインプログラムパッケージのサイズが表示されます。ダウンロードされたパッケージは<サーバのインストールフォルダ>¥PCCSRV¥Download¥Product に保存されます。

ダウンロードされたパッケージは<サーバのインストールフォルダ>¥PCCSRV¥Download¥Product に保存されます。

ダウンロード中は進行状況を監視することも、別の画面に移動することもできます。

注意

パッケージのダウンロードまたはインストール中に問題が発生した場合は、Web コンソールでサーバアップデートログを確認します。メインメニューで、[ログ] > [サーバアップデート] の順にクリックします。

3. [インストール] または [後でインストール] をクリックします。

   - [インストール] をクリックすると、インストールが開始され、インストールの進行状況画面が表示されます。
   - [後でインストール] をクリックすると、[プラグインマネージャ] 画面が表示されます。

     プラグインプログラムをインストールするには、[プラグインマネージャ] 画面のプラグインプログラムのセクションにある [インストール] ボタンをクリックします。

   トレンドマイクロの使用許諾契約書画面が表示されます。

   注意

   プラグインプログラムによってはこの画面は表示されず、すぐにプラグインプログラムのインストールが開始されます。

4. [同意する] をクリックしてプラグインプログラムをインストールします。

   インストール中は進行状況を監視することも、別の画面に移動することもできます。

注意

パッケージのダウンロードまたはインストール中に問題が発生した場合は、Web コンソールでサーバアップデートログを確認します。メインメニューで、[ログ] > [サーバアップデート] の順にクリックします。

インストールが終了すると、現在のプラグインプログラムのバージョンが[プラグインマネージャ] 画面に表示されます。

プラグインプログラムライセンスのアクティベート

手順

1. Apex One Web コンソールを開いて、メインメニューで [プラグイン] をクリックします。
2. [プラグインマネージャ] 画面で、プラグインプログラムのセクションに移動し、[プログラムの管理] をクリックします。

   [製品ライセンスの新しいアクティベーションコード] 画面が表示されます。
3. アクティベーションコードをテキストフィールドに入力するか、コピーして貼り付けます。
4. [保存] をクリックします。

   プラグインコンソールが表示されます。

ライセンス情報の表示と更新

手順

1. Apex One Web コンソールを開いて、メインメニューで [プラグイン] をクリックします。
2. [プラグインマネージャ] 画面で、プラグインプログラムのセクションに移動し、[プログラムの管理] をクリックします。

3. プラグインコンソールで [ライセンス情報の表示] をクリックします。

   [ライセンス情報の表示] ハイパーリンクはプラグインプログラムによって表示される場所が異なります。詳細については、プラグインプログラムのユーザマニュアルを参照してください。

4. 表示された画面でライセンスに関する次の詳細を確認します。

オプション	説明
ステータス	[アクティベーション完了]、[アクティベーション未完了]、または [サポート契約終了] と表示されます。
バージョン	[製品版] または [体験版] バージョンのいずれかが表示されます。 **注意** 製品版と体験版の両方がアクティベートされている場合、「製品版」とのみ表示されます。
ライセンス有効期限	プラグインプログラムに複数のライセンスがある場合、最も遅い有効期限が表示されます。 たとえば、サポート契約の有効期限が 2010 年 12 月 31 日と 2010 年 6 月 30 日の場合は、2010 年 12 月 31 日が表示されます。
アクティベーションコード	アクティベーションコードが表示されます。
注意事項	現在のライセンスバージョンに応じて、更新猶予期間中 (製品版のみ) またはライセンスの有効期限が切れたときに、ライセンスの有効期限に関するメッセージが表示されます。

注意

プラグインプログラムの更新猶予期間については、トレンドマイクロの販売代理店にお問い合わせください。

ライセンスの有効期限が切れた後もプラグインプログラムは引き続き使用できますが、アップデートおよびサポートは利用できません。

5. トレンドマイクロの Web サイトで現在のライセンスに関する情報を確認するには、[詳細情報をオンラインで確認] をクリックします。

6. 画面を最新のライセンス情報に更新するには、[ステータスをオンラインで確認] をクリックします。
7. [製品ライセンスの新しいアクティベーションコード] をクリックして、[製品ライセンスの新しいアクティベーションコード] 画面を開きます。

   詳細については、86 ページの「プラグインプログラムライセンスのアクティベート」を参照してください。

プラグインプログラムの管理

Web コンソールからアクセスできるプラグインプログラムの管理コンソールで設定を行って、プログラム関連タスクを実行します。プログラムのアクティベートやエージェントへのプラグインプログラムの配信などのタスクがあります。特定のプラグインプログラムの設定と管理の詳細については、プログラムのドキュメントを参照してください。

プラグインプログラムの管理

手順

1. Apex One Web コンソールを開いて、メインメニューで [プラグイン] をクリックします。
2. [プラグインマネージャ] 画面で、プラグインプログラムのセクションに移動し、[プログラムの管理] をクリックします。

   プラグインプログラムは、初回の管理時にアクティベーションが必要になることがあります。詳細については、86 ページの「プラグインプログラムライセンスのアクティベート」を参照してください。

プラグインプログラムのバージョンアップ

プラグインマネージャコンソールには、インストールされているプラグインプログラムの新しいバージョンが表示されます。このコンソールで、パッケージをダウンロードし、プラグインプログラムをバージョンアップします。

バージョンアップパッケージは、プラグインマネージャによってトレンドマイクロのアップデートサーバまたはユーザ指定のアップデート元 (正しく設定されている場合) からダウンロードされます。トレンドマイクロのアップデートサーバからパッケージをダウンロードするには、インターネット接続が必要です。

プラグインマネージャによってインストールパッケージがダウンロードされるか、バージョンアップが開始されると、他のプラグインプログラムのダウンロード、インストール、バージョンアップなどの機能は一時的に使用できなくなります。

プラグインマネージャは、Apex Central のシングルサインオン機能によるプラグインプログラムのバージョンアップをサポートしていません。

プラグインプログラムのバージョンアップ

手順

1. Apex One Web コンソールを開いて、メインメニューで [プラグイン] をクリックします。
2. [プラグインマネージャ] 画面で、プラグインプログラムのセクションに移動し、[ダウンロード] をクリックします。

   [ダウンロード] ボタンの横に、バージョンアップパッケージのサイズが表示されます。

   ダウンロード中は進行状況を監視することも、別の画面に移動することもできます。

   注意

   パッケージのダウンロードまたはインストール中に問題が発生した場合は、Web コンソールでサーバアップデートログを確認します。メインメニューで、[ログ] > [サーバアップデート] の順にクリックします。
3. パッケージがダウンロードされると、新しい画面が表示されます。
4. [今すぐバージョンアップ] または [後でバージョンアップ] をクリックします。

- [今すぐバージョンアップ] をクリックすると、バージョンアップが開始され、バージョンアップの進行状況画面が表示されます。
- [後でバージョンアップ] をクリックすると、[プラグインマネージャ] 画面が表示されます。

  プラグインプログラムをバージョンアップするには、[プラグインマネージャ] 画面のプラグインプログラムのセクションにある [バージョンアップ] ボタンをクリックします。

バージョンアップの後、プラグインマネージャサービスの再起動が必要な場合があります。再起動中、[プラグインマネージャ] 画面が一時的に使用できなくなります。[プラグインマネージャ] 画面が使用可能になると、現在のプラグインプログラムのバージョンが表示されます。

プラグインプログラムのアンインストール

次の方法でプラグインプログラムをアンインストールします。

- プラグインマネージャコンソールからプラグインプログラムをアンインストールします。
- Apex One サーバをアンインストールします。これによって、プラグインマネージャおよびインストールされているすべてのプラグインプログラムがアンインストールされます。Apex One サーバをアンインストールする手順については、「*Apex One インストールガイド*」を参照してください。

エンドポイント上にエージェントがあるプラグインプログラムについては、次の点に注意してください。

- プラグインプログラムのドキュメントを参照して、プラグインプログラムをアンインストールするとプラグインエージェントもアンインストールされるかどうかを確認してください。
- セキュリティエージェントと同じエンドポイントにインストールされたプラグインエージェントについては、セキュリティエージェントをアンインストールすると、プラグインエージェントとセキュリティエージェ

ントプラグインマネージャ (CNTAoSMgr.exe) もアンインストールされます。

プラグインマネージャコンソールからのプラグインプログラムのアンインストール

手順

1. Apex One Web コンソールを開いて、メインメニューで [プラグイン] をクリックします。
2. [プラグインマネージャ] 画面で、プラグインプログラムのセクションに移動し、[アンインストール] をクリックします。
3. アンインストール中は進行状況を監視します。または、別の画面に移動することもできます。
4. アンインストール後に [プラグインマネージャ] 画面を更新します。

   アンインストールしたプログラムが再びインストール可能になります。

プラグインマネージャのアンインストール

プラグインマネージャおよびインストールされているすべてのプラグインプログラムをアンインストールするには、Apex One サーバをアンインストールします。Apex One サーバをアンインストールする手順については、「*Apex One インストールガイド*」を参照してください。

プラグインマネージャのトラブルシューティング

Apex One サーバとセキュリティエージェントのデバッグログを確認して、プラグインマネージャとプラグインプログラムのデバッグ情報を調べてください。

プラグインプログラムがプラグインマネージャコンソールに表示されない

ダウンロードおよびインストール可能なプラグインプログラムがプラグインマネージャコンソールに表示されない場合、次のような原因が考えられます。

手順

1. プラグインマネージャはプラグインプログラムをまだダウンロードしていますが、プログラムのパッケージサイズが大きいと時間がかかる場合があります。時々画面をチェックして、プラグインプログラムが表示されているかどうか確認してください。

   注意

   プラグインプログラムをダウンロードできなかった場合は、24 時間後に自動的にダウンロードが再度行われます。プラグインマネージャを手動で起動してプラグインプログラムをダウンロードするには、Apex One プラグインマネージャサービスを再起動します。

2. サーバコンピュータがインターネットに接続できません。サーバがプロキシサーバ経由でインターネットに接続する場合は、そのプロキシ設定でインターネット接続を確立できることを確認してください。

3. Apex One のアップデート元がトレンドマイクロのアップデートサーバではありません。Apex One Web コンソールで、[アップデート] > [サーバ] > [アップデート元] に移動して、アップデート元を確認してください。アップデート元がトレンドマイクロのアップデートサーバでない場合は、次のオプションを選択できます。

   - アップデート元としてトレンドマイクロのアップデートサーバを選択します。
   - [その他のアップデート元] を選択している場合は、[その他のアップデート元] リスト内の最初のエントリをアップデート元として選択し、そのアップデート元がトレンドマイクロのアップデートサーバに正常に接続できることを確認します。プラグインマネージャは、リストの最初のエントリのみをサポートします。

- [現在のファイルのコピーを含むイントラネットの場所] を選択している場合は、イントラネット内のエンドポイントもトレンドマイクロのアップデートサーバに接続できることを確認します。

エンドポイントでのプラグインエージェントのインストールと表示に関する問題

エンドポイントでのプラグインプログラムのエージェントのインストールに失敗する場合や、プラグインプログラムのエージェントがセキュリティエージェントコンソールに表示されない場合、次のような原因が考えられます。

手順

1. エンドポイント上のエージェントプラグインマネージャ (CNTAosMgr.exe) が実行されていません。セキュリティエージェントエンドポイントで、Windows のタスクマネージャを開いて、CNTAosMgr.exe プロセスを実行します。

2. プラグインエージェントのインストールパッケージが、<エージェントインストールフォルダ>¥AU_Data¥AU_Temp¥{xxx}AU_Down¥Product にあるセキュリティエージェントエンドポイントフォルダにダウンロードされていません。¥AU_Data¥AU_Log¥にある Tmudump.txt を確認して、ダウンロードに失敗した原因を調べてください。

   注意

   エージェントが正常にインストールされた場合は、<エージェントインストールフォルダ>¥AOSSvcInfo.xml でエージェント情報を参照できます。

3. エージェントのインストールに失敗したか、さらに操作が必要です。プラグインプログラムの管理コンソールでインストールステータスを確認し、必要な操作 (インストール後にセキュリティエージェントエンドポイントを再起動する、必須 OS パッチをインストールしてからインストールするなど) を行います。

Internet Explorer の自動構成スクリプトがプロキシサーバへリダイレクトするように設定されている場合、エンドポイント上のエージェントを起動できない

エージェント起動コマンドがプロキシサーバへリダイレクトされるため、セキュリティエージェントプラグインマネージャ (CNTAosMgr.exe) はエンドポイント上のエージェントを起動できません。この問題はプロキシ設定がユーザの HTTP トラフィックを 127.0.0.1 へリダイレクトするように設定されている場合にのみ発生します。

この問題を解決するには、適切に定義されたプロキシサーバポリシーを使用します。たとえば、HTTP トラフィックを 127.0.0.1 へ切り替えないでください。

HTTP 要求を 127.0.0.1 へ制御するプロキシ設定を使用する必要がある場合は、次のタスクを実行します。

手順

1. Apex One Web コンソールで Apex One ファイアウォールの設定を行います。

   注意

   この手順を実行するのは、セキュリティエージェントで Apex One ファイアウォールが有効になっている場合のみです。

   a. Web コンソールで、[エージェント] > [ファイアウォール] > [ポリシー] に移動し、[除外テンプレートの編集] をクリックします。

   b. [除外テンプレートの編集] 画面で、[追加] をクリックします。

   c. 次の情報を使用します。

      - 名前: 希望する名前
      - 処理: ネットワークトラフィックを許可
      - 方向: 受信

- プロトコル: TCP
- ポート: 5000～49151 のポート番号

d. IP アドレス: [単一 IP アドレス] を選択し、プロキシサーバの IP アドレスを指定します (推奨)。または、[すべての IP アドレス] を選択します。

e. [保存]をクリックします。

f. [除外テンプレートの編集] 画面に戻り、[保存してすべての既存ポリシーに適用] をクリックします。

g. [エージェント] > [ファイアウォール] > [プロファイル] に移動し、[エージェントにプロファイルを適用] をクリックします。

ファイアウォールプロファイルがない場合は、[追加] をクリックして作成します。次の設定を使用します。

- 名前: 希望する名前
- 説明: 希望する説明
- ポリシー: オールアクセスポリシー

新しく作成したプロファイルを保存したら、[エージェントにプロファイルを適用] をクリックします。

2. `ofcscan.ini` ファイルを変更します。

a. テキストエディタを使用して、<サーバインストールフォルダ>内の `ofcscan.ini` ファイルを開きます。

b. `[Global Setting]` を含む行を検索して、その下の行に「`FWPortNum=21212`」を追加します。「21212」は、上記の手順 c で指定したポート番号に変更してください。

例:

```
[Global Setting]

FWPortNum=5000
```

c. ファイルを保存します。

3. Web コンソールで、[エージェント] > [グローバルエージェント設定] に移動し、[保存] をクリックします。

システム、アップデートモジュール、またはプラグインマネージャプログラムでエラーが発生し、特定のエラーコードがエラーメッセージに表示される

プラグインマネージャでエラーメッセージに表示されるエラーコードは次のとおりです。次の表に記載されている解決策を参照しても問題を解決できない場合は、サポート担当者にお問い合わせください。

表 17-1. プラグインマネージャのエラーコード

エラーコード	メッセージ、原因、および解決策
001	プラグインマネージャプログラムでエラーが発生しました。 アップデートタスクの進行状況を照会しても、プラグインマネージャのアップデートモジュールが応答しません。アップデートモジュールまたはコマンドハンドラが初期化されていない可能性があります。 Apex One プラグインマネージャサービスを再起動し、もう一度タスクを実行してください。

エラーコード	メッセージ、原因、および解決策
002	システムエラーが発生しました。 プラグインマネージャのアップデートモジュールは、レジストリキー SOFTWARE\TrendMicro\OfficeScan\service\AoS を開けません。レジストリキーが削除されている可能性があります。 次の手順を実行します。 1. レジストリエディタを開いて、HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_Addon_Service_CompList_Version に移動します。値を 1.0.1000 に設定し直します。 2. Apex One プラグインマネージャサービスを再起動します。 3. プラグインプログラムをダウンロードまたはアンインストールします。

エラーコード	メッセージ、原因、および解決策
028	アップデートエラーが発生しました。 次の原因が考えられます。 • プラグインマネージャのアップデートモジュールがプラグインプログラムをダウンロードできませんでした。ネットワーク接続が機能しているかどうかを確認して、再度実行してください。 • AU パッチエージェントからエラーが返されたため、プラグインマネージャのアップデートモジュールはプラグインプログラムをインストールできません。AU パッチエージェントは、新しいプラグインプログラムのインストールを開始するプログラムです。エラーの具体的な原因については、\PCCSRV\Web\Service\AU_Data\AU_Log にあるアップデートモジュールのデバッグログ「TmuDump.txt」を確認してください。 次の手順を実行します。 1. レジストリエディタを開いて、HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_Addon_Service_CompList_Version に移動します。値を 1.0.1000 に設定し直します。 2. プラグインプログラムのレジストリキー HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_ADDON_xxxx を削除します。 3. Apex One プラグインマネージャサービスを再起動します。 4. プラグインプログラムをダウンロードしてインストールします。
170	システムエラーが発生しました。 プラグインマネージャのアップデートモジュールは、新しく要求された処理を実行できません。現在、別の処理を実行しています。 時間を置いてタスクを実行してください。

エラーコード	メッセージ、原因、および解決策
202	プラグインマネージャプログラムでエラーが発生しました。 プラグインマネージャプログラムは、Web コンソールで実行中のタスクを処理できません。 Web コンソールの表示を更新するか、プラグインマネージャをバージョンアップしてください (可能な場合)。
203	プラグインマネージャプログラムでエラーが発生しました。 プラグインマネージャのバックエンドサービスと通信しようとした際に、プラグインマネージャプログラムでプロセス間通信 (IPC) エラーが発生しました。 Apex One プラグインマネージャサービスを再起動し、もう一度タスクを実行してください。
その他のエラーコード	システムエラーが発生しました。 新しいプラグインプログラムをダウンロードする際、プラグインマネージャは、トレンドマイクロのアップデートサーバのプラグインプログラムリストをチェックします。プラグインマネージャでこのリストを取得できませんでした。 次の手順を実行します。 1. レジストリエディタを開いて、`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_Addon_Service_CompList_Version` に移動します。値を `1.0.1000` に設定し直します。 2. Apex One プラグインマネージャサービスを再起動します。 3. プラグインプログラムをダウンロードしてインストールします。

第 18 章

トラブルシューティングのリソース

この章では、Apex One サーバのトラブルシューティングと、セキュリティエージェントの問題において使用できるリソースのリストを提供します。

この章は次のトピックで構成されます。

インテリジェントシステムのサポート

インテリジェントシステムのサポートページを使用すると、分析用のファイルをトレンドマイクロに簡単に送信できます。このシステムでは、Apex One サーバの GUID が特定され、分析ファイルとともに送信されます。Apex One サーバの GUID を知ることで、トレンドマイクロでは、診断のために送られてきたファイルに関するフィードバックを提供できます。

ケース診断ツール

トレンドマイクロのケース診断ツール (cdt) は、問題が発生した場合にお客さまの製品から必要なデバッグ情報を収集します。製品のデバッグステータスをオンまたはオフに自動的に切り替えて、問題のカテゴリに従って必要なファイルを収集します。トレンドマイクロはこの情報を使用して、製品に関連する問題をトラブルシューティングします。

Apex One でサポートされるすべてのプラットフォームでツールを実行します。このツールと使用方法については、下記ページをご確認ください。
https://success.trendmicro.com/jp/solution/1313294

Trend Micro パフォーマンス調整ツール

トレンドマイクロでは、潜在的にパフォーマンスの問題を引き起こす可能性があるアプリケーションを特定する、スタンドアロンのパフォーマンス調整ツールを用意しています。Trend Micro パフォーマンス調整ツールは、テストインストール時にスタンドアロンのワークステーションのイメージや少数のインストール先ワークステーションで実行し、挙動監視およびデバイスコントロールを実際にインストールする前に、パフォーマンスの問題を解決します。

詳細については、https://success.trendmicro.com/jp/solution/1310435 を参照してください。

注意

多くの場合、パフォーマンスの問題はより複雑な問題が原因で発生します。パフォーマンス低下の根本原因を特定できない場合は、サポート担当者にお問い合わせください。

Apex One サーバログ

Web コンソールで利用可能なログだけでなく、その他の種類のログ (デバッグログなど) も、製品の問題に対するトラブルシューティングに使用できます。

警告!

デバッグログはサーバの性能に影響を与え、大量のディスク空き容量を消費する可能性があります。必要なときにのみデバッグログ生成を有効にし、デバッグデータが不要になった場合はただちに無効にしてください。ディスク容量を節約する必要がある場合は、ログファイルを削除してください。

LogServer.exe を使用するサーバデバッグログ

`LogServer.exe` を使用して以下に対するデバッグログを収集します。

- Apex One サーバの基本ログ
- トレンドマイクロ脆弱性検索ツール
- Active Directory 統合ログ
- エージェントのグループ設定ログ
- セキュリティコンプライアンスログ
- 役割ベースの管理
- スマートスキャン

デバッグログ

Apex One は「エラー」イベントに関連するデバッグログを自動的に収集します。デバッグログの収集を無効にしようとすると、Apex One は「エラー」ログの収集を自動的に再開します。

手順

1. Web コンソールにログオンします。
2. Web コンソールのバナーで、「Trend Micro Apex One」の「T」をクリックします。
3. [デバッグログを有効にする] をオンにします。

   注意

   デバッグログの収集を無効にしようとすると、Apex One は「エラー」ログの収集を自動的に再開します。

4. デバッグログ設定を指定します。

   注意

   Apex One は「エラー」イベントに関連するデバッグログを自動的に収集します。デバッグログの収集を無効にしようとすると、Apex One は「エラー」ログの収集を自動的に再開します。

5. [保存] をクリックします。
6. 次の初期設定の場所にあるログファイル (`ofcdebug.log`) をチェックします。<サーバインストールフォルダ>¥PCCSRV¥Log

サーバのインストールとバージョンアップのデバッグログの有効化

次のタスクを実行する前に、デバッグログを有効にします。

- サーバをアンインストールして、再度インストールする。

- Apex One を最新バージョンにバージョンアップする。
- リモートインストール/バージョンアップを実行する (デバッグログはセットアップを起動したコンピュータでのみ有効となり、リモートコンピュータには適用されません)。

手順

1. <サーバインストールフォルダ>¥PCCSRV¥Private にある [LogServer] フォルダを C:¥にコピーします。
2. ofcdebug.ini という名前のファイルを作成し、次の内容を入力します。

   ```
   [debug]

   debuglevel=9

   debuglog=c:¥LogServer¥ofcdebug.log

   debugLevel_new=D

   debugSplitSize=10485760

   debugSplitPeriod=12

   debugRemoveAfterSplit=1
   ```

3. ofcdebug.ini を C:¥LogServer に保存します。
4. 適切なタスクを実行します (サーバのアンインストール/再インストール、新しいサーババージョンへのバージョンアップ、またはリモートでのインストール/バージョンアップ)。
5. C:¥LogServer の ofcdebug.log を確認します。

インストールログ

- ローカルインストール/バージョンアップログ

  ファイル名: OFCMAS.LOG

  場所: %windir%

Active Directory ログ

- ファイル名: `ofcdebug.log`
- ファイル名: `ofcserver.ini`

  場所:<サーバインストールフォルダ>`¥PCCSRV¥Private¥`

役割ベースの管理ログ

役割ベースの管理に関する詳細情報を取得するには、次のいずれかを実行します。

- トレンドマイクロのケース診断ツールを実行します。詳細については、776 ページの「ケース診断ツール」を参照してください。
- 次のログを収集します。
  - <サーバインストールフォルダ>`¥PCCSRV¥Private¥AuthorStore` フォルダ内のすべてのファイル
  - 777 ページの「Apex One サーバログ」

セキュリティエージェントのグループ設定ログ

- ファイル名: `ofcdebug.log`
- ファイル名:`ofcserver.ini`

  場所:<サーバインストールフォルダ>`¥PCCSRV¥Private¥`
- ファイル名: `SortingRule.xml`

  場所: <サーバインストールフォルダ>`¥PCCSRV¥Private ¥SortingRuleStore¥`

コンポーネントアップデートログ

ファイル名:`TmuDump.txt`

場所:<サーバインストールフォルダ>¥PCCSRV¥Web¥Service¥AU_Data¥AU_Log

サーバのアップデート情報詳細の取得

手順

1. aucfg.ini という名前のファイルを作成し、次の内容を入力します。

   ```
   [Debug]

   level=-1

   [Downloader]

   ProxyCache=0
   ```

2. ファイルを <サーバインストールフォルダ>¥PCCSRV¥Web¥Service に保存します。
3. Apex One Master Service を再起動します。

サーバのアップデート情報詳細の取得の中止

手順

1. aucfg.ini を削除します。
2. Apex One Master Service を再起動します。

エージェントパッケージャログ

エージェントパッケージャ作成ログの有効化

手順

1. <サーバインストールフォルダ>¥PCCSRV¥Admin¥Utility ¥ClientPackager にある ClnExtor.ini ファイルを次のように変更します。

   ```
   [Common]

   DebugMode=1
   ```

2. C:¥の ClnPack.log を確認します。

エージェントパッケージャ作成ログの無効化

手順

1. ClnExtor.ini ファイルを開きます。
2. [DebugMode] 値を 1 から 0 に変更します。

セキュリティコンプライアンスレポートログ

詳細なセキュリティコンプライアンス情報を取得するには、次の情報を収集します。

- ファイル名:RBAUserProfile.ini

  場所:<サーバインストールフォルダ>¥PCCSRV¥Private¥AuthorStore¥

- <サーバインストールフォルダ>¥PCCSRV¥Log¥Security Compliance Report フォルダ内のすべてのファイル
- 777 ページの「Apex One サーバログ」

外部サーバ管理ログ

- ファイル名:ofcdebug.log
- ファイル名:ofcserver.ini

  場所:<サーバインストールフォルダ>¥PCCSRV¥Private¥
- <サーバインストールフォルダ>¥PCCSRV¥Log¥Outside Server Management Report¥フォルダ内のすべてのファイル

デバイスコントロール除外ログ

詳細なデバイスコントロール除外情報を取得するには、次の情報を収集します。

- ファイル名:ofcscan.ini

  場所:<サーバインストールフォルダ>¥
- Apex One Web コンソールのデバイスコントロール除外リスト

統合 Smart Protection Server の Web レピュテーションログ

ファイル名:diagnostic.log

場所:<サーバインストールフォルダ>¥PCCSRV¥LWCS¥

ServerProtect 一般サーバ移行ツールログ

ServerProtect 一般サーバ移行ツールのデバッグログのデバッグログ生成を有効にするには:

手順

1. ofcdebug.ini という名前のファイルを作成し、次の内容を入力します。

   [Debug]

```
DebugLog=C:¥ofcdebug.log

DebugLevel=9
```

2. ファイルを C:¥に保存します。
3. C:¥の ofcdebug.log を確認します。

注意

デバッグログを無効にするには、ofcdebug.ini ファイルを削除します。

VSEncrypt ログ

Apex One は自動的にデバッグログ (VSEncrypt.log) をユーザアカウントの一時フォルダ内に作成します。たとえば、C:¥Documents and Settings¥<ユーザ名>¥Local Settings¥Temp フォルダに作成します。

Apex Central MCP エージェントデバッグログ

<サーバインストールフォルダ>¥PCCSRV¥CMAgent フォルダに次のデバッグファイルが作成されます。

- Agent.ini
- Product.ini
- [Apex Central 設定] ページのスクリーンショット
- ProductUI.zip

MCP エージェントのデバッグログの有効化

手順

1. <サーバインストールフォルダ>¥PCCSRV¥CmAgent 内の product.ini ファイルを次のように修正します。

```
[Debug]
```

```
debugmode = 3

debuglevel= 3

debugtype = 0

debugsize = 10000

debuglog = C:\CMAgent_debug.log
```

2. Apex One Apex Central Agent サービスを Microsoft 管理コンソールから再起動します。
3. C:¥の CMAgent_debug.log を確認します。

MCP エージェントのデバッグログの無効化

手順

1. product.ini ファイルを開いて次の行を削除します。

```
debugmode = 3

debuglevel= 3

debugtype = 0

debugsize = 10000

debuglog = C:\CMAgent_debug.log
```

2. Apex One Apex Central Agent サービスを再起動します。

アウトブレークログ

検索の種類	ファイル
現在のファイアウォール違反アウトブレークログ	ファイル名:Cfw_Outbreak_Current.log 場所:<サーバインストールフォルダ>¥PCCSRV¥Log¥

検索の種類	ファイル
前回のファイアウォール違反アウトブレークログ	ファイル名:Cfw_Outbreak_Last.log 場所: <サーバインストールフォルダ>¥PCCSRV¥Log¥
現在のウイルス/不正プログラムのアウトブレークログ	ファイル名:Outbreak_Current.log 場所: <サーバインストールフォルダ>¥PCCSRV¥Log¥
前回のウイルス/不正プログラムのアウトブレークログ	ファイル名:Outbreak_Last.log 場所: <サーバインストールフォルダ>¥PCCSRV¥Log¥
現在のスパイウェア/グレーウェアアウトブレークログ	ファイル名:Spyware_Outbreak_Current.log 場所: <サーバインストールフォルダ>¥PCCSRV¥Log¥
前回のスパイウェア/グレーウェアアウトブレークログ	ファイル名:Spyware_Outbreak_Last.log 場所: <サーバインストールフォルダ>¥PCCSRV¥Log¥

Trend Micro VDI オプションログ

- ファイル名: vdi_list.ini

  場所:<サーバインストールフォルダ>¥PCCSRV¥TEMP¥

- ファイル名:vdi.ini

  場所: <サーバインストールフォルダ>¥PCCSRV¥Private¥

- ファイル名: ofcdebug.txt

  場所: <サーバインストールフォルダ>¥PCCSRV¥Log

ofcdebug.txt を生成するには、デバッグログを有効にします。デバッグログを有効にする手順については、778 ページの「デバッグログ」を参照してください。

セキュリティエージェントログ

セキュリティエージェントの問題のトラブルシューティングにセキュリティエージェントログ (デバッグログなど) を使用できます。

警告!

デバッグログはエージェントパフォーマンスに影響し、大量のディスク空き容量を消費する可能性があります。必要なときにのみデバッグログ生成を有効にし、デバッグデータが不要になった場合はただちに無効にしてください。ファイルサイズが巨大になった場合はログファイルを削除してください。

LogServer.exe を使用するセキュリティエージェントのデバッグログ

セキュリティエージェントのデバッグログを有効にする手順は次のとおりです。

手順

1. LogServer フォルダの内容 (Log サブフォルダを除く) を対象エンドポイントの新しい場所にコピーします。

   LogServer フォルダは次の場所にあります。

   - 新しいセキュリティエージェントの場合: `C:¥Program Files (x86)¥Trend Micro¥Security Agent¥Temp¥LogServer¥`
   - アップグレードしたセキュリティエージェントの場合: `C:¥Program Files (x86)¥Trend Micro¥OfficeScan Client¥Temp¥LogServer¥`
   - Apex One サーバの場合: `¥Program Files (x86)¥Trend Micro¥Apex One¥PCCSRV¥Private¥LogServer`

2. LogServer¥ofcdebug.ini ファイルの内容を次のように変更します。

   ```
   Debuglog=C:\ofcdebug.log

   debugLevel_new=D
   ```

ForceStopOtherLogserver=1

最大スプリットサイズを初期設定の 10MB よりも大きくする場合には、debugSplitSize=10485760 を変更します。

ログファイルの最大数を変更する場合には、DebugMaxSplit=100 を変更します。

3. ファイルを保存します。
4. 対象エンドポイントで、LogServer.exe を [管理者として実行] します。

   ツールにより、ofcdebug.log ファイルが作成されます。
5. 問題を再現します。
6. LogServer.exe の画面を閉じて、デバッグログの収集を中止します。
7. デバッグログの収集中に作成されたログファイル (.log と .7z) をすべて、別の場所に移します。
8. 手順 1 でコピーしたファイルをすべて削除します。

新規インストールログ

MSI パッケージインストールの場合:

- ファイル名: OFCNT.LOG
- 場所: 一時システムファイル。Windows 7 の例:

  C:¥Users¥Administrator¥AppData¥Local¥Trend Micro¥Security Agent¥OFCNT.LOG

Web インストールの場合:

- ファイル名: WebInstall.log
- 場所: C:¥

リモートインストールの場合:

- ファイル名: RemoteInstall.LOG

- 場所: C:¥

Autopcc と EXE パッケージによるインストールの場合:

- ファイル名: OFCNT.LOG
- 場所: %windir%¥

バージョンアップ/HotFix ログ

ファイル名:upgrade_yyyymmddhhmmss.log

場所:<エージェントインストールフォルダ>¥Temp

ダメージクリーンナップサービスデバッグログ

ダメージクリーンナップサービスのデバッグログの有効化

手順

1. <エージェントインストールフォルダ> にある TSC.ini ファイルを開きます。
2. 次の行を以下のように修正してください。

   DebugInfoLevel=5

3. <エージェントインストールフォルダ>¥debug の TSCDebug.log を確認します。

ダメージクリーンナップサービスのデバッグログの無効化

TSC.ini ファイルを開いて「DebugInfoLevel」の値を 5 から 0 に変更します。

クリーンナップログ

ファイル名:yyyymmdd.log

場所:<エージェントインストールフォルダ>¥report¥

メール検索ログ

ファイル名:SmolDbg.txt

場所:<エージェントインストールフォルダ>

セキュリティエージェント接続ログ

ファイル名:Conn_YYYYMMDD.log

場所:<エージェントインストールフォルダ>¥ConnLog

セキュリティエージェントアップデートログ

ファイル名:Tmudump.txt

場所:<エージェントインストールフォルダ>¥AU_Data¥AU_Log

セキュリティエージェントのアップデート情報詳細の取得

手順

1. aucfg.ini という名前のファイルを作成し、次の内容を入力します。

```
[Debug]
level=-1
[Downloader]
ProxyCache=0
```

2. ファイルを <エージェントインストールフォルダ> に保存します。
3. セキュリティエージェントを再起動します。

注意

エージェントのアップデート情報詳細の取得を中止するには、aucfg.ini ファイルを削除し、セキュリティエージェントを再起動します。

ウイルス検索エンジンログ

ウイルス検索エンジンのデバッグログ生成を有効にするには:

手順

1. レジストリエディタ (regedit.exe) を開きます。
2. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMFilter\Parameters を開きます。
3. [DebugLogFlags] の値を「00003eff」に変更します。
4. 表示される検索問題に沿って手順を実行します。
5. %windir%の TMFilter.log を確認します。

注意

デバッグログを無効にするには、[DebugLogFlags] の値を「00000000」に戻します。

大規模感染予防サービスログ

ファイル名:OPPLogs.log

場所:<エージェントインストールフォルダ>¥OppLog

大規模感染予防サービス復元ログ

ファイル名:

- TmOPP.ini
- TmOPPRestore.ini

場所:<エージェントインストールフォルダ>¥

挙動監視のデバッグログ

挙動監視のデバッグログを有効にするには

手順

1. レジストリエディタ (regedit.exe) を開きます。
2. HKLM\SOFTWARE\TrendMicro\Aegis に移動します。
3. キー「DebugLogFlags」を「dword:00000032」として追加します。
4. 問題が発生した手順を再現します。
5. C:¥Program Files (x86)¥Trend Micro¥BM¥log¥フォルダにある次のログを確認します。
   - TmCommengyyyymmdd_nn.log
   - TMPEMyyyymmdd_nn.log

Apex One ファイアウォールログ

一般的なファイアウォールドライバのデバッグログの有効化 (すべての OS の場合)

手順

1. 次のレジストリの値を変更します。

レジストリキー	値
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmwfp\Parameters	**種類:** DWORD 値 (REG_DWORD) **名前:** DebugCtrl **値:** 0x00001111
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmlwf\Parameters	**種類:** DWORD 値 (REG_DWORD) **名前:** DebugCtrl **値:** 0x00001111

2. エンドポイントを再起動します。
3. C:¥の wfp_log.txt および lwf_log.txt を確認します。

一般的なファイアウォールドライバのデバッグログの無効化 (すべての OS の場合)

手順

1. レジストリキーの [DebugCtrl] を削除します。
2. エンドポイントを再起動します。

Apex One NT ファイアウォールサービスのデバッグログの有効化

手順

1. <エージェントインストールフォルダ> にある TmPfw.ini ファイルを次のように編集します。

   ```
   [ServiceSession]

   Enable=1
   ```

2. セキュリティエージェントを再起動します。
3. C:¥temp の ddmmyyyy_NSC_TmPfw.log を確認します。

Apex One NT ファイアウォールサービスのデバッグログの無効化

手順

1. TmPfw.ini ファイルを開き、「Enable」の値を 1 から 0 に変更します。
2. セキュリティエージェントを再起動します。

Web レピュテーションおよび POP3 メール検索のログ

Web レピュテーション機能と POP3 メール検索機能のデバッグログの有効化

手順

1. <エージェントインストールフォルダ> にある TmOsprey.ini ファイルを次のように編集します。

   ```
   [InteractiveSession]

   Enable=1
   ```

```
LogFolder=C:\temp

[ServiceSession]

Enable=1

LogFolder=C:\temp
```

2. セキュリティエージェントを再起動します。
3. C:¥temp の yyyy-mm-dd_hh-mm-ss_EE_TmOsprey1.etl を確認します。

Web レピュテーション機能と POP3 メール検索機能のデバッグログの無効化

手順

1. <エージェントインストールフォルダ> にある TmOsprey.ini ファイルを次のように編集します。

```
[InteractiveSession]

Enable=0

LogFolder=C:\temp

[ServiceSession]

Enable=0

LogFolder=C:\temp
```

2. セキュリティエージェントを再起動します。

デバイスコントロール除外リストログ

ファイル名:DAC_ELIST

場所:<エージェントインストールフォルダ>¥

注意

暗号化されたログデータにアクセスする方法は、サポート担当者にお問い合わせください。

情報漏えい対策オプションデバッグログ

情報漏えい対策オプションデバッグログを有効にするには

手順

1. サポートセンターから `logger.cfg` ファイルを入手します。
2. `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite` に、次のデータを追加します。
   - 種類: `String`
   - 名前: `debugcfg`
   - 値: `C:¥Log¥logger.cfg`
3. `C:¥`ディレクトリに、「Log」という名前のフォルダを作成します。
4. `Log` フォルダに `logger.cfg` をコピーします。
5. Web コンソールから情報漏えい対策とデバイスコントロールの設定を配信して、ログの収集を開始します。

注意

情報漏えい対策オプションモジュールのデバッグログを無効にするには、レジストリキーの `debugcfg` を削除し、エンドポイントを再起動します。

Windows イベントログ

Windows イベントビューアには、ログオンやアカウント設定の変更など、正常に実行されたアプリケーションイベントが記録されます。

手順

1. 次のいずれかを実行します。
   - [スタート] > [コントロール パネル] > [パフォーマンスとメンテナンス] > [管理ツール] > [コンピュータの管理] の順にクリックします。
   - イベントビューアスナップインを含む MMC を開きます。
2. [イベント ビューア] をクリックします。

転送ドライバインタフェース (TDI) デバッグログ

転送ドライバインタフェース (TDI) デバッグログを有効にするには

手順

1. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\tmtdi\Parameters に、次のデータを追加します。

パラメータ	値
キー 1	**種類:** DWORD **値** (REG_DWORD) **名前:**Debug **値:**1111 (16 進数)
キー 2	**種類:**String 値 (REG_SZ) **名前:**LogFile **値:**C:¥tmtdi.log

2. エンドポイントを再起動します。
3. C:¥の tmtdi.log を確認します。

注意

TDI のデバッグログを無効にするには、レジストリキーの `Debug` と `LogFile` を削除し、エンドポイントを再起動します。

第 19 章

テクニカルサポート

ここでは、次の項目について説明します。

トラブルシューティングのリソース

トレンドマイクロでは以下のオンラインリソースを提供しています。テクニカルサポートに問い合わせる前に、こちらのサイトも参考にしてください。

サポートポータルの利用

サポートポータルでは、よく寄せられるお問い合わせや、障害発生時の参考となる情報、リリース後に更新された製品情報などを提供しています。

https://success.trendmicro.com/jp/technical-support

脅威データベース

現在、不正プログラムの多くは、コンピュータのセキュリティプロトコルを回避するために、2 つ以上の技術を組み合わせた複合型脅威で構成されています。トレンドマイクロは、カスタマイズされた防御戦略を策定した製品で、この複雑な不正プログラムに対抗します。脅威データベースは、既知の不正プログラム、スパム、悪意のある URL、および既知の脆弱性など、さまざまな混合型脅威の名前や兆候を包括的に提供します。

詳細については、https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/ をご覧ください。

- 現在アクティブまたは「in the Wild」と呼ばれている生きた不正プログラムと悪意のあるモバイルコード
- これまでの Web 攻撃の記録を記載した、相関性のある脅威の情報ページ
- 対象となる攻撃やセキュリティの脅威に関するオンライン勧告
- Web 攻撃およびオンラインのトレンド情報
- 不正プログラムの週次レポート

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

トレンドマイクロの Web サイトでは、ネットワークを脅かすウイルスやセキュリティに関する最新の情報を公開しています。ウイルスが検出された場合や、最新のウイルス情報を知りたい場合などにご利用ください。

サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「製品サポートガイド」または「スタンダードサポートサービスメニュー」をご覧ください。

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話またはお問い合わせ Web フォームをご利用ください。サポートセンターの連絡先は、「製品サポートガイド」または「スタンダードサポートサービスメニュー」に記載されています。

サポート契約の有効期限は、ユーザ登録完了から 1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、サポートサービス継続を希望される場合は契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意

サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出/駆除できない場合などに、感

染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。

ファイルを送信いただく前に、トレンドマイクロの不正プログラム情報検索サイト「脅威データベース」にアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/

ファイルを送信いただく場合は、次の URL にアクセスして、サポートセンターの受付フォームからファイルを送信してください。

https://success.trendmicro.com/jp/virus-and-threat-help

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

メールレピュテーションについて

スパムメールやフィッシングメールなどの送信元を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

ファイルレピュテーションについて

不正プログラムなどのファイル情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

Web レピュテーションについて

不正な Web サイトや URL などの情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

製品やドキュメントの最新版は、次の Web ページからダウンロードできます。

https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

注意

サービス製品、販売代理店経由での販売製品、または異なる提供形態をとる製品など、一部対象外の製品があります。

脅威解析・サポートセンター TrendLabs (トレンドラボ)

TrendLabs (トレンドラボ) は、フィリピン・米国に本部を置き、日本・台湾・ドイツ・アイルランド・中国・フランス・イギリス・ブラジルの 10 カ国 12 か所の各国拠点と連携してソリューションを提供しています。

世界中から選び抜かれた 1,000 名以上のスタッフで 24 時間 365 日体制でインターネットの脅威動向を常時監視・分析しています。

付録

付録

付録 A

Apex One の IPv6 のサポート

本付録は、Apex One を IPv6 アドレス指定をサポートする環境にインストールするユーザにお読みいただく必要があります。本付録では、Apex One での IPv6 のサポートに関する情報をのみを提供します。

IPv6 の概念、および IPv6 アドレス指定をサポートするネットワークの設定作業に詳しいユーザを対象読者としています。

Apex One サーバおよびエージェントでの IPv6 のサポート

IPv6 の要件を満たす Apex One サーバおよびセキュリティエージェントをインストールまたはバージョンアップすると、IPv6 のサポートが自動的に有効になります。

Apex One サーバの要件

Apex One サーバにおける IPv6 の要件は次のとおりです。

- サーバが IPv4 と IPv6 のセキュリティエージェントを管理する場合は、サーバに IPv4 と IPv6 の両方のアドレスを割り当てて、ホスト名で識別する必要があります。IPv4 アドレスでサーバを識別すると、IPv6 セキュリティエージェントはそのサーバに接続できません。IPv4 シングルスタックエージェントが、IPv6 アドレスで識別されたサーバに接続する場合も、同じ問題が発生します。
- サーバが IPv6 エージェントのみを管理する場合は、IPv6 アドレスを使用することが最低要件となります。サーバは、ホスト名または IPv6 アドレスによって識別できます。サーバをホスト名で識別する場合は、完全修飾ドメイン名 (FQDN) を使用することをお勧めします。これは、IPv6 シングルスタックの環境では、WINS サーバがホスト名をそれに対応する IPv6 アドレスに変換できないためです。

注意

FQDN は、サーバのローカルインストールを実行する場合にのみ指定できます。これは、リモートインストールではサポートされていません。

IPv6 シングルスタックサーバの制限事項

次の表は、Apex One サーバに IPv6 アドレスのみが割り当てられている場合の制限事項のリストです。

表 A-1. IPv6 シングルスタックサーバの制限事項

項目	制限事項
エージェント管理	IPv6 シングルスタックサーバでは次の作業を行うことができません。 • IPv4 シングルスタックエンドポイントへのセキュリティエージェントの導入 • IPv4 シングルスタックのセキュリティエージェントの管理
アップデートと一元管理	IPv6 シングルスタックサーバを、次のような IPv4 シングルスタックのアップデート元からアップデートすることはできません。 • トレンドマイクロのアップデートサーバ • IPv4 シングルスタックのユーザ指定のアップデート元
製品の登録、アクティベーション、およびサポート契約更新	IPv6 シングルスタックサーバは、トレンドマイクロのオンライン登録サーバに接続して、製品の登録、ライセンスの取得、およびライセンスのアクティベート/サポート契約の更新を行うことはできません。
プロキシ接続	IPv6 シングルスタックサーバは、IPv4 シングルスタックプロキシサーバ経由で接続することはできません。
プラグインソリューション	IPv6 シングルスタックサーバにはプラグインマネージャがインストールされますが、次の対象にプラグインソリューションを配信することはできません。 • IPv4 シングルスタックのセキュリティエージェントまたは IPv4 シングルスタックホスト (直接接続がないため) • IPv6 シングルスタックのセキュリティエージェントまたは IPv6 シングルスタックホスト (いずれのプラグインソリューションも IPv6 をサポートしていないため)

これらの制限事項のほとんどは、IPv4 アドレスと IPv6 アドレスを変換できる DeleGate などのデュアルスタックプロキシサーバを設定することで克服できます。Apex One サーバと接続先のエンティティまたは処理対象のエンティティとの間にプロキシサーバを配置してください。

IPv6 シングルスタックのセキュリティエージェントの制限事項

次の表は、IPv6 アドレスのみ指定されているセキュリティエージェントの制限事項を示しています。

表 A-2. IPv6 シングルスタックエージェントの制限事項

項目	制限事項
上位 Apex One サーバ	IPv6 シングルスタックセキュリティエージェントは、IPv4 シングルスタックの Apex One サーバでは管理できません。
アップデート	IPv6 シングルスタックエージェントは、IPv4 シングルスタックの次のアップデート元からはアップデートできません。 • トレンドマイクロのアップデートサーバ • IPv4 シングルスタックの Apex One サーバ • IPv4 シングルスタックのアップデートエージェント • IPv4 シングルスタックのその他のアップデート元
検索クエリ、Web レピュテーションクエリ、およびスマートフィードバック	IPv6 シングルスタックセキュリティエージェントからは、次のような Smart Protection ソースにクエリを送信することはできません。 • Trend Micro Smart Protection Network (スマートフィードバックも含む)
ソフトウェアの安全性	IPv6 シングルスタックのセキュリティエージェントは、トレンドマイクロがホストするソフトウェア安全性評価サービスに接続できません。
プラグインソリューション	いずれのプラグインソリューションも IPv6 をサポートしていないため、IPv6 シングルスタックのセキュリティエージェントでプラグインソリューションをインストールすることはできません。
プロキシ接続	IPv6 シングルスタックセキュリティエージェントは、IPv4 シングルスタックのプロキシサーバを介して接続できません。

これらの制限事項の多くは、IPv4 アドレスと IPv6 アドレスを変換できる DeleGate などのデュアルスタックプロキシサーバを設定することで回避でき

ます。プロキシサーバは、セキュリティエージェントと接続先との間に設置します。

IPv6 アドレスを設定する

Web コンソールを使用して、IPv6 アドレスまたは IPv6 のアドレス範囲を設定できます。設定のガイドラインを次にいくつか示します。

- Apex One では、標準の IPv6 アドレス表記がサポートされます。

  例を以下に示します。

  ```
  2001:0db7:85a3:0000:0000:8a2e:0370:7334
  ```

  ```
  2001:db7:85a3:0:0:8a2e:370:7334
  ```

  ```
  2001:db7:85a3::8a2e:370:7334
  ```

  ```
  ::ffff:192.0.2.128
  ```

- Apex One では、次の例に示すようなリンクローカルの IPv6 アドレスもサポートされます。

  ```
  fe80::210:5aff:feaa:20a2
  ```

  警告!

  Apex One ではリンクローカルの IPv6 アドレスがサポートされますが、状況によっては予期したとおりに動作しない場合もあるため、リンクローカルの IPv6 アドレスを指定する際には注意が必要です。たとえば、アップデート元が別のネットワークセグメント上にあり、それがリンクローカルの IPv6 アドレスで識別される場合、セキュリティエージェントではそのアップデート元からアップデートできません。

- IPv6 アドレスが URL の一部である場合は、アドレスを角カッコ ([]) で囲みます。
- IPv6 のアドレス範囲では、通常、プレフィックス長を入力する必要があります。サーバで IP アドレスのクエリを実行する必要のある設定では、サーバが大量の IP アドレスについてクエリを実行する際に発生する可能性のあるパフォーマンス上の問題を回避するため、プレフィックス長

の制限が適用されます。たとえば、外部サーバ管理機能の場合、プレフィックスの長さは 112 (65,536 個の IP アドレス) から 128 (2 個の IP アドレス) でなければなりません。

- IPv6 アドレスまたはアドレス範囲に関する設定には、セキュリティエージェントに配信されても無視されるものがあります。たとえば、Trend Micro Smart Protection ソースリストを設定しており、IPv6 アドレスで識別された Smart Protection Server がリストに含まれている場合、IPv4 セキュリティエージェントはそのサーバを無視して、他の Trend Micro Smart Protection ソースに接続します。

IP アドレスが表示される画面

ここでは、IP アドレスが表示される Web コンソール内の場所を紹介します。

場所	説明
エージェントツリー	エージェントツリーが表示されると、[IP アドレス] 列に IPv6 シングルスタックのセキュリティエージェントの IPv6 アドレスが表示されます。デュアルスタックのセキュリティエージェントについては、サーバへの登録時に IPv6 アドレスを使用した場合に IPv6 アドレスが表示されます。 **注意** サーバへの登録時にデュアルスタックのセキュリティエージェントが使用する IP アドレスは、[エージェント] > [グローバルエージェント設定] の [ネットワーク] > [優先 IP アドレス] で制御できます。 エージェントツリーの設定をファイルにエクスポートすると、エクスポートしたファイルにも IPv6 アドレスが表示されます。
エージェントステータス	[エージェント] > [エージェント管理] の [ステータス] に移動すると、詳細なエージェント情報を参照できます。この画面には、IPv6 シングルスタックのセキュリティエージェントおよびサーバへの登録時に IPv6 アドレスを使用した、デュアルスタックのセキュリティエージェントの IPv6 アドレスが表示されます。

場所	説明
ログ	次のログにデュアルスタックおよび IPv6 シングルスタックのセキュリティエージェントの IPv6 アドレスが表示されます。 • ウイルス/不正プログラムログ • スパイウェア/グレーウェアログ • ファイアウォールログ • 接続状態の確認ログ
Apex Central コンソール	以下は、Apex Central コンソールに表示される Apex One サーバおよびセキュリティエージェントの IP アドレスのリストです。 • デュアルスタックサーバ:IPv4 および IPv6 • IPv4 シングルスタックサーバ:IPv4 • IPv6 シングルスタックサーバ:IPv6 • デュアルスタックセキュリティエージェント:セキュリティエージェントが Apex One サーバに登録されるときに使用した IP アドレス • IPv4 シングルスタックセキュリティエージェント:IPv4 • IPv6 シングルスタックセキュリティエージェント:IPv6

付録 B

Windows Server Core のサポート

この付録では、Apex One における Windows Server Core のサポート状況について説明します。

Windows Server Core のサポート

Windows Server Core は Windows Server バージョンの「最小」インストールです。Server Core には次の特長があります。

- Windows Server のオプションと機能の多くが削除されています。
- サーバでは、非常に軽量な主要部分のみの OS を実行できます。
- タスクは主にコマンドラインインタフェースから実行します。
- 起動時に実行されるサービス数が少なく、必要なリソースも少量です。

Apex One では、次のバージョンの Windows Server Core へのセキュリティエージェントのインストールをサポートしています。

- Windows Server Core 2008 R2
- Windows Server Core 2012
- Windows Server Core 2012 R2
- Windows Server Core 2016
- Windows Server Core 2019

セキュリティエージェントは Server Core をサポートしています。ここでは、Server Core に対するサポート範囲について説明します。

Apex One サーバは Server Core をサポートしていません。

Windows Server Core のインストール方法

次のインストール方法については、一部または全部がサポートされていません。

- Web インストールページ: Server Core では Web ブラウザを使用できないため、この方法はサポートされていません。
- トレンドマイクロ脆弱性検索ツール:脆弱性検索ツールを Server Core でローカル実行することはできません。このツールは Apex One サーバまたは別のエンドポイントから実行してください。

次のインストール方法がサポートされています。

- リモートインストール。詳細については、150 ページの「Apex One Web コンソールからのリモートインストール」を参照してください。
- ログオンスクリプトウィザード
- エージェントパッケージャ

ログオンスクリプトウィザードを使用したセキュリティエージェントのインストール

手順

1. 対象エンドポイントで、コマンドプロンプトを開きます。
2. 次のコマンドを入力して、Apex One サーバの `AutoPcc.exe` ファイルの場所をマップします。

   `net use <マップするドライブ文字> \\<Apex One サーバのホスト名または IP アドレス>\ofcscan`

   例:

   `net use P:\\10.1.1.1\ofcscan`
3. 対象サーバのユーザ名とパスワードを入力します。

   `AutoPcc.exe` の場所が正常にマップされたかどうかを示すメッセージが表示されます。
4. マップされたドライブ文字とコロン「:」を入力して、`AutoPcc.exe` の場所に移動します。例:

   `P:`
5. 以下を入力してインストールを開始します。

   `AutoPcc.exe`

   インストールが完了すると新しいコマンドプロンプトが表示されます。

セキュリティエージェントパッケージを使用したセキュリティエージェントのインストール

手順

1. パッケージを作成します。

   詳細については、155 ページの「エージェントパッケージャを使用したインストール」を参照してください。

2. コマンドプロンプトを開きます。

3. 次のコマンドを入力して、セキュリティエージェントパッケージの場所をマップします。

   ```
   net use <マップするドライブ文字> \\<エージェントパッケージの場所>
   ```

   例:

   ```
   net use P:\\10.1.1.1\Package
   ```

   セキュリティエージェントパッケージの場所が正常にマップされたかどうかを示すメッセージが表示されます。

4. マップされたドライブ文字とコロン「:」を入力して、セキュリティエージェントパッケージの場所に移動します。例:

   ```
   P:
   ```

5. 次のコマンドを入力して、セキュリティエージェントパッケージを Server Core エンドポイントのローカルディレクトリにコピーします。

   ```
   copy <パッケージファイル名> <パッケージをコピーする Server Core エンドポイントのディレクトリ>
   ```

   例:

   ```
   copy securityagent.msi C:\Agent Package
   ```

   セキュリティエージェントパッケージが正常にコピーされたかどうかを示すメッセージが表示されます。

6. ローカルディレクトリに移動します。例:

```
C:

cd C:\Agent Package
```

7. パッケージファイル名を入力して、インストールを開始します。例:

   ```
   securityagent.msi
   ```

   コマンドプロンプトに入力するコマンドとその結果は、次のようになります。

   ```
   C:\WINDOWS>net use P: \\10.1.1.1\Package
   C:\Windows>P:
   P:\>copy securityagent.msi C:\Agent Package
           1 file(s) copied.
   P:\>C:
   C:\WINDOWS>cd C:\Agent Package
   C:\Agent Package>securityagent.msi
   ```

Windows Server Core でのセキュリティエージェント機能

サポート対象のバージョンの Windows Server で利用できるセキュリティエージェント機能のほとんどが、Server Core でも利用できます。サポートされていない機能は、スタンドアロンモードのみです。

Windows Server で利用できる機能のリストについては、137 ページの「セキュリティエージェントの機能」を参照してください。

セキュリティエージェントコンソールには、コマンドラインインタフェースからのみアクセス可能です。

注意

一部のセキュリティエージェントコンソール画面には [ヘルプ] ボタンがあり、クリックすると HTML ベースの状況に応じたヘルプが表示されます。Windows Server Core にはブラウザがないため、このヘルプを使用できません。ヘルプを表示するにはブラウザをインストールする必要があります。

Windows Server Core のコマンド

コマンドラインインタフェースからコマンドを実行して、セキュリティエージェントのタスクを実行します。

コマンドを実行するには、「PccNTMon.exe」がある場所に移動します。このプロセスによって、セキュリティエージェントコンソールが起動します。このプロセスは<エージェントインストールフォルダ>にあります。

次の表に使用可能なコマンドを示します。

表 B-1. Windows Server Core のコマンド

コマンド	処理
pccnt <ドライブまたはフォルダパス>	指定したドライブまたはフォルダでセキュリティリスクを検索します。 ガイドライン: • フォルダパスにスペースが含まれる場合は、パス全体を引用符で囲みます。 • ファイルを個々に検索することはできません。 正しいコマンド: • pccnt C:¥ • pccnt D:\Files • pccnt "C:\Documents and Settings" 正しくないコマンド: • pccnt C:¥Documents and Settings • pccnt D:¥Files¥example.doc
pccntmon -r	リアルタイムモニタを開きます。
pccntmon -v	エージェントコンポーネントとそのバージョンを表示します。
pccntmon -u	セキュリティエージェントコンポーネントをアップデートします。

コマンド	処理
pccntmon -n <アンロードパスワード>	セキュリティエージェントをアンロードします。 セキュリティエージェントを再ロードするには、次のコマンドを入力します。 pccntmon
pccntmon -m <アンインストールパスワード>	セキュリティエージェントをアンインストールします。

pccntmon -c	コマンドラインに次の情報が表示されます。
	• 検索方法
	  • スマートスキャン
	  • 従来型スキャン
	• パターンファイルのステータス
	  • 最新版
	  • 旧版
	• リアルタイム検索サービス
	  • 機能しています
	  • 無効または機能していません
	• エージェントの接続状態
	  • オンライン
	  • スタンドアロン
	  • オフライン
	• Web レピュテーションサービス
	  • 利用可能
	  • 再度接続しています
	• ファイルレピュテーションサービス
	  • 使用可能
	  • 再接続しています

コマンド	処理
`pccntmon -h`	使用可能なすべてのコマンドを表示します。

付録 C

用語集

この用語集では、よく参照されるエンドポイント用語、およびトレンドマイクロ製品やテクノロジの詳細について説明します。

アップデート

アップデートは、多くのトレンドマイクロ製品に共通の機能です。トレンドマイクロのアップデート Web サイトに接続すると、アップデートによって、パターンファイル、検索エンジン、プログラム、その他のトレンドマイクロコンポーネントファイルの最新のダウンロードが、インターネット経由で提供されます。

圧縮ファイル

1 つまたは複数の個別ファイルと情報を含む単一のファイルで、WinZip などの対応プログラムで展開できます。

Cookie

名前、傾向、関心事など、インターネットユーザに関する情報を格納するメカニズム。この情報は、後から使用できるように Web ブラウザに格納されます。ブラウザに cookie が保存されている Web サイトに次回アクセスすると、ブラウザは cookie を Web サーバに送信します。Web サーバはその cookie を使用して、カスタマイズされた Web ページを表示できます。たとえば、名前を表示してユーザを受け入れる Web サイトにアクセスする場合などです。

サービス拒否攻撃

サービス拒否 (DoS) 攻撃は、「サービス」、つまりネットワーク接続の中断を発生させるエンドポイントまたはネットワークに対する攻撃のことを指します。通常、DoS 攻撃は、ネットワーク帯域幅に悪影響を与えたり、エンドポイントのメモリなどのシステムリソースをオーバーロードさせます。

DHCP

DHCP (Dynamic Host control Protocol) は、動的 IP アドレスをネットワーク内のデバイスに割り当てるためのプロトコルです。動的アドレス指定によ

り、デバイスは、ネットワークに接続するたびに異なる IP アドレスを持つことができます。一部のシステムでは、デバイスの IP アドレスは、ネットワークに接続中でも変更できます。DHCP では、静的 IP アドレスと動的 IP アドレスの混在もサポートします。

DNS

ドメインネームシステム (DNS) は、ホスト名を IP アドレスに変換するために主にインターネットで使用される汎用的なデータクエリサービスです。

DNS エージェントが、DNS サーバにホスト名とアドレスデータを要求するときのプロセスは、解決と呼ばれます。基本的な DNS 設定では、サーバは初期設定の解決プロセスを実行します。たとえばリモートサーバは、現在のゾーンにあるコンピュータのデータについて、別のサーバに問い合わせます。リモートサーバ上のエージェントソフトウェアはリゾルバに問い合わせます。リゾルバは、データベースファイルからの要求に応答します。

ドメイン名

`tellsitall.com` のようにローカルホスト名とドメイン名で構成されるシステムの完全名。ドメイン名は、インターネット上の任意のホストに対して一意のインターネットアドレスを特定できるものである必要があります。「名前解決」と呼ばれるこのプロセスでは、ドメインネームシステム (DNS) を使用します。

動的 IP アドレス

動的 IP アドレスは、DHCP サーバが割り当てる IP アドレスです。エンドポイントの MAC アドレスは固定ですが、IP アドレスについては、空き状況に応じて DHCP サーバにより新しいアドレスがエンドポイントに割り当てられることがあります。

ESMTP

拡張簡易メール転送プロトコル (ESMTP) の適用範囲には、帯域幅の節約とサーバの保護を実現するためのセキュリティ、認証、および他のデバイスが含まれています。

使用許諾契約書

使用許諾契約書あるいは EULA は、ソフトウェア発行者とソフトウェアのユーザの間の法的な契約です。一般的には、ユーザ側の制限について説明したもので、ユーザはインストール時に [同意します] をクリックしなければ契約の締結を拒否できます。もちろん [同意しません] ボタンをクリックした場合は、ソフトウェア製品のインストールは中止されます。

悪意のあるフリーソフトのインストールの際に表示される [使用許諾契約書] ウィンドウで、うっかり [同意します] をクリックしてしまい、スパイウェアやその他の種類のグレーウェアをユーザのコンピュータにインストールすることに同意してしまうことがよくあります。

誤検出

ファイルが感染していると誤ってセキュリティソフトウェアで検出されたときに、誤検出は発生します。

FTP

ファイル転送プロトコル (FTP) は、インターネットを介して、ファイルをサーバからクライアントへ転送する際に使用される標準プロトコルです。詳細については、Network Working Group の RFC 959 を参照してください。

Generic Clean

Generic Clean は、ウイルスクリーンナップコンポーネントが使用可能でなくても不正プログラムを駆除することができる新技術です。検出済みのファイルを基準に、Generic Clean は、そのファイルに対応するプロセス/サービスがメモリおよびレジストリ内にあるかどうかを判定し、該当するものを一斉に削除します。

HotFix

HotFix とは、お客さま固有の問題に対する修正プログラムです。HotFix は、お客さま固有の問題に対応するものであるため、すべてのお客さまに配布されるものではありません。

初期設定では、セキュリティエージェントには HotFix がインストールされます。HotFix をセキュリティエージェントにインストールしたくない場合は、Web コンソールにおいて、[エージェント] > [エージェント管理] に移動し、[設定] > [権限とその他の設定] > [その他の設定] タブでエージェントのアップデート設定を変更してください。

HTTP

ハイパーテキスト転送プロトコル (HTTP) はインターネットを介して、グラフィックやマルチメディアコンテンツを含む Web ページをサーバからクライアントへ転送する際に使用される標準プロトコルです。

HTTPS

SSL (Secure Socket Layer) を使用するハイパーテキスト転送プロトコル。HTTPS は、セキュリティで保護されたトランザクションの処理に使用される HTTP の変形です。

ICMP

ゲートウェイあるいは宛先のホストとソースホスト間の通信において、ICMP (Internet Control Message Protocol) を使用する場合があります。たとえば、データグラムプロセスにおけるエラー通知などです。ICMP は IP の基本的サポートを上位のプロトコルであるかのように使用しますが、ICMP は実際には IP の不可欠な部分で、各 IP モジュールに実装されています。ICMP メッセージはさまざまな状況で送信されます。たとえば、データグラムが宛先に届かない場合、ゲートウェイのバッファ容量がデータグラム転送に必要な容量に不足している場合、より短いルートでトラフィックを送信するようにゲートウェイがホストに指示できる場合などです。インターネットプロトコルは、信頼性が完全であるように設計されていません。これらのコントロールメッセージの目的は、通信環境における問題に対するフィードバックを提供することで、IP の信頼性を高めることではありません。

トレンドマイクロの推奨設定

トレンドマイクロの推奨設定は、検索するファイルを特定する方法です。実行可能ファイル (`.exe` など) では、ファイルの種類はファイルの内容に基づいて判断されます。その他のファイルの種類 (`.txt` など) は、ファイルのヘッダに基づいて判断されます。

トレンドマイクロの推奨設定には、次の利点があります。

- パフォーマンスの最適化: トレンドマイクロの推奨設定は、最小限のシステムリソースを使用するため、エージェントのアプリケーションには影響しません。
- 検索時間の短縮: トレンドマイクロの推奨設定では実際のファイルタイプを識別するため、感染の危険性があるファイルだけが検索されます。そのため、すべてのファイルを検索する場合に比べ、検索時間が大幅に短縮されます。

IntelliTrap

ウイルス作成者は、リアルタイム圧縮のアルゴリズムを使用して、ウイルスフィルタを回避しようとすることがあります。IntelliTrap は、リアルタイム

の圧縮済み実行ファイルを遮断し、他の不正プログラムの特性とファイルを組み合わせて、ユーザのネットワークに入り込むというようなウイルスのリスクを減らすのに役立っています。IntelliTrap は、このようなファイルをセキュリティリスクと見なし、安全なファイルを誤ってブロックする場合があるため、IntelliTrap を有効にするときは、ファイルを削除または消去せずに隔離することを検討してください。ユーザが定期的にリアルタイムの圧縮された実行ファイルをやりとりする場合は、IntelliTrap を無効にします。

IntelliTrap では、以下のコンポーネントを使用します。

- ウイルス検索エンジン
- IntelliTrap パターンファイル
- IntelliTrap 除外パターンファイル

IP

「インターネットプロトコル (IP) は、データグラムと呼ばれるデータブロックの送信を送信元から宛先へ提供する。そこでの送信元と宛先は、固定長アドレスによって識別されるホストである。」(RFC 791)

Java ファイル

Java は、Sun Microsystems によって開発された汎用プログラミング言語です。Java ファイルは Java コードを含みます。Java は、プラットフォームに依存しない Java「アプレット」の形式で、インターネットのプログラミングをサポートします。アプレットは、HTML ページに挿入できる、Java プログラミング言語で記述されたプログラムです。Java 技術対応のブラウザを使用してアプレットを含むページを表示すると、アプレットのコードはエンドポイントに転送され、ブラウザの Java 仮想マシンでアプレットが実行されます。

LDAP

LDAP (Lightweight Directory Access Protocol) は、TCP/IP 上で動作するディレクトリサービスの問い合わせおよび変更を行うアプリケーションプロトコルです。

待機ポート

待機ポートは、データ交換のためのエージェント接続要求に利用されます。

MCP エージェント

MCP (Trend Micro Management Communication Protocol) は、管理対象製品用のトレンドマイクロの次世代エージェントです。MCP は TMI (Trend Micro Management Infrastructure) に代わり、Apex Central と Apex One 間の通信に利用されます。MCP には多くの新しい機能があります。

- ネットワークの負荷とパッケージサイズの削減
- NAT とファイアウォールの横断サポート
- HTTPS のサポート
- 一方向/双方向通信サポート
- シングルサインオン (SSO) のサポート
- クラスタノードのサポート

複合型の脅威の攻撃

複合型の脅威の攻撃は、企業のネットワークにある複数の侵入ポイントと脆弱性を利用します。このような脅威の攻撃には、「Nimda」や「Code Red」などがあります。

NAT

ネットワークアドレス変換 (NAT) は、セキュリティで保護された IP アドレスを、アドレスプールにある一時的な外部の登録 IP アドレスに変換するための規格です。これにより、非公開に IP アドレスが割り当てられた信頼するネットワークが、インターネットにアクセスできるようになります。つまり、ネットワーク内のすべてのコンピュータに対応する登録 IP アドレスを取得する必要はありません。

NetBIOS

ネットワーク基本入出力システム (NetBIOS) は、ネットワーク機能などの機能をディスクオペレーティングシステム (DOS) の基本入出力システム (BIOS) に追加するアプリケーションプログラムインタフェース (API) です。

一方向通信

NAT 妨害は現在のネットワーク環境でますます重要な問題になっています。この問題に取り組むために、MCP では一方向通信を用いています。一方向通信では、MCP エージェントがサーバとの接続を開始し、コマンドをやりとりします。それぞれの要求は、CGI に似たコマンドクエリまたはログ伝送です。ネットワークへの影響を軽減するために、接続を維持し、できる限り開放しています。その後の要求は、既存の開いた接続を使用します。接続が切断されると、同じホストに対する SSL 接続はすべてセッション ID キャッシュのメリットを利用して、再接続時間を大幅に短縮します。

Patch

Patch とは、HotFix と Critical Patch が 1 つにまとめられたもので、複数の問題を解決します。トレンドマイクロは、定期的に Patch を公開しています。Windows 版の Patch にはセットアッププログラムが含まれますが、Windows 版以外の Patch には通常、セットアップスクリプトが用意されています。

フィッシング攻撃

フィッシュあるいはフィッシングは、急速に増加している詐欺形式の 1 つで、合法的な Web サイトを装って、Web ユーザの個人情報を暴露するものです。

典型的なシナリオでは、ユーザが突然驚くような (本物にしか見えない) メールを受け取ります。内容は、「口座に問題が発生して、ただちに口座解約を回避する手続きが必要である」という内容です。メールにはいかにも本物らしく見える Web サイトへの URL が記載されています。本物のメールと本物の Web サイトをコピーするのは簡単ですが、収集されたデータを受信するいわゆるバックエンドを変更するのも簡単です。

メールはサイトにログオンしてアカウント情報を確認するようにユーザに指示します。ユーザが提供する、ログオン名、パスワード、クレジットカード番号などのデータをハッカーは受け取ります。

フィッシング詐欺は費用をかけずに手軽に実行でき、簡単に継続できます。これはまた、犯人にとってお金儲けにつながる可能性があります。フィッシングはコンピュータに詳しいユーザでさえ検出が難しいのです。これは法的に規制するのも容易ではありません。さらに悪いことに、起訴することはほとんど不可能です。

フィッシングサイトの疑いがある Web サイトを発見したときは、トレンドマイクロに報告してください。

Ping

Ping は、IP アドレスに対して ICMP エコー要求を送信し、応答を待つユーティリティです。Ping ユーティリティは、指定した IP アドレスを持つエンドポイントがオンラインかどうかを決定します。

POP3

POP3 (Post Office Protocol 3) は、サーバからのメールメッセージを格納し、クライアントのメールアプリケーションへ転送する標準プロトコルです。

プロキシサーバ

特殊な接頭辞が付いた URL を受け入れる WWW サーバ。ローカルキャッシュまたはリモートサーバのいずれかから文書を取得するために使用され、その URL を要求元に返します。

RPC

リモートプロシージャコール (RPC) は、あるホストで動作するプログラムがコードを別のホストで実行させることができるようにするネットワークプロトコルです。

Critical Patch

Critical Patch とは、セキュリティ上の問題に対応するもので、すべてのお客さまに対して公開されます。Windows 版の Critical Patch にはセットアッププログラムが含まれますが、Windows 版以外の Critical Patch には通常、セットアップスクリプトが用意されています。

Service Pack

Service Pack とは、HotFix と Patch が統合され、大幅な機能拡張が含まれている修正プログラムで、製品のバージョンアップに相当します。Windows 版および Windows 版以外の Service Pack のどちらにも、セットアッププログラムとセットアップスクリプトが含まれます。

SMTP

簡易メール転送プロトコル (SMTP) は、インターネットを介して、メールメッセージをサーバからサーバおよびエージェントからサーバに転送するために使用する標準プロトコルです。

snmp

簡易ネットワーク管理プロトコル (SNMP) は、管理上注意すべき状態について、ネットワークに接続されているデバイスの管理をサポートするプロトコルです。

SNMP トラップ

SNMP (Small Network Management Protocol) トラップは、SNMP プロトコルをサポートする管理コンソールを使用しているネットワーク管理者に通知を送信する方法です。

Apex One では、通知を管理情報ベース (MIB) に格納できます。MIB ブラウザを使用して、SNMP トラップ通知を表示できます。

SSL

SSL (Secure Socket Layer) は、アプリケーションプロトコル (HTTP、Telnet、FTP など) と TCP/IP の間に層をなすデータセキュリティを提供するため、Netscape によって設計されたプロトコルです。このセキュリティプロトコルは、データの暗号化、サーバの認証、メッセージの完全性、および任意の TCP/IP 接続のエージェント認証を実現します。

SSL 証明書

セキュリティで保護された HTTPS 通信を確立するデジタル証明書です。

TCP

伝送制御プロトコル (TCP) は、マルチネットワークアプリケーションをサポートするプロトコルの階層に対応するように設計された、接続志向のエンドツーエンドの信頼性のあるプロトコルです。TCP は IP データグラムを利

用してアドレス解決を行います。詳細については、DARPA インターネットプログラムの RFC 793 を参照してください。

Telnet

Telnet は「ネットワーク仮想端末」を作成して、端末デバイスを TCP に接続させる標準的な方法です詳細については、Network Working Group の RFC 854 を参照してください。

トロイの木馬に脆弱なポート

トロイの木馬に脆弱なポートとは、一般にトロイの木馬プログラムがエンドポイントへの接続に使用するポートのことです。大規模感染が発生した場合、Apex One ではトロイの木馬プログラムが使用する可能性がある次の番号のポートがブロックされます。

表 C-1. トロイの木馬に脆弱なポート

ポート番号	トロイの木馬プログラム	ポート番号	トロイの木馬プログラム
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM

ポート番号	トロイの木馬プログラム	ポート番号	トロイの木馬プログラム
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

信頼されたポート

サーバとセキュリティエージェントは、信頼されたポートを使用して互いに通信します。

信頼されたポートをブロックし、大規模感染後にネットワーク設定を通常の状態に戻しても、セキュリティエージェントはサーバとの通信をただちに再開しません。エージェントとサーバの通信は、[大規模感染予防の設定] 画面で指定した時間が経過してからでないと、元に戻りません。

Apex One では、HTTP ポート (初期設定では 8080) をサーバの信頼されたポートとして使用します。インストール中に、別のポート番号を入力できます。この信頼されたポートと、セキュリティエージェント上の信頼されたポートをブロックするには、[ブロックされるポート] 画面で [信頼されたポートをブロック] チェックボックスをオンにします。

マスターインストーラは、インストール中にセキュリティエージェントの信頼されたポートをランダムに生成します。

信頼されたポートの特定

手順

1. <サーバインストールフォルダ>¥PCCSRV にアクセスします。
2. メモ帳などのテキストエディタを使用して、ofcscan.ini を開きます。
3. サーバの信頼されたポートについては、文字列「Master_DomainPort」を検索し、その横の値を確認します。

   たとえば、Master_DomainPort=80 という文字列がある場合は、サーバの信頼されたポートはポート 80 であることを示します。
4. エージェントの信頼されたポートについては、文字列「Client_LocalServer_Port」を検索し、その横の値を確認します。

   たとえば、Client_LocalServer_Port=41375 という文字列がある場合は、エージェントの信頼されたポートはポート 41375 であることを示します。

双方向通信

双方向通信は、一方向通信に代わる方法です。双方向通信は一方向通信に基づいていますが、サーバ通知を受信する HTTP ベースのチャネルが追加されています。双方向通信では、MCP エージェントによる、サーバからのコマンドのリアルタイムな送信と処理が向上します。

UDP

ユーザデータグラムプロトコル (UDP) は、アプリケーションプログラムが他のプログラムにメッセージを送信するために、IP とともに使用されるコネク

ションレス通信です。詳細については、DARPA インターネットプログラムの RFC 768 を参照してください。

ウイルス駆除できないファイル

ウイルス検索エンジンは、以下のファイルを駆除できません。

表 C-2. 駆除できないファイルの解決策

駆除できないファイル	説明と解決策
トロイの木馬に感染したファイル	トロイの木馬は、メッセージの表示、ファイルの消去、ディスクのフォーマットなど、予期しない、または許可されていない一般に不正な処理を実行するプログラムです。トロイの木馬はファイルに感染しないため駆除は必要はありません。 解決策: ダメージクリーンナップエンジンとダメージクリーンナップテンプレートを使用してトロイの木馬を削除します。
ワームに感染したファイル	ワームは、ワーム自体またはその一部の動作可能なコピーを他のエンドポイントシステムに拡散できる自己完結型プログラムまたはプログラムのセットです。伝播には通常、ネットワーク接続やメールの添付ファイルが利用されます。ワームはファイルが自己完結型プログラムであるため駆除できません。 解決策:トレンドマイクロではワームを削除することをお勧めします。
書き込み保護された感染ファイル	解決策: ファイルを駆除できるよう書き込み保護を解除します。
パスワード保護されたファイル	パスワード保護されたファイルには、パスワード保護された圧縮ファイルや Microsoft Office ファイルが含まれます。 解決策: ファイルを駆除できるようパスワード保護を解除します。
バックアップファイル	RB0～RB9 のような拡張子を持つファイルは感染ファイルのバックアップコピーです。駆除処理中にウイルス/不正プログラムによってファイルが破壊された場合に備えて、駆除処理では感染ファイルのバックアップを作成します。 解決策: 正常に駆除された場合、感染ファイルのバックアップコピーを残しておく必要はありません。エンドポイントが通常どお

駆除できないファイル	説明と解決策
	り機能している場合は、バックアップファイルを削除してもかまいません。
ごみ箱の感染ファイル	システムが稼働中のため、ごみ箱から感染ファイルを削除できない場合があります。
	1. エンドポイントに管理者権限でログオンします。 2. アプリケーションがファイルをロックし、Windows で削除できなくなることを防止するため、実行中のアプリケーションをすべて閉じます。 3. コマンドプロンプトを開きます。 4. 次を入力してファイルを削除します。 `del /s \$Recycle.Bin\*` 5. ファイルが削除されたかどうか確認します。
Windows の一時フォルダまたは Internet Explorer の一時フォルダ内の感染ファイル	エンドポイントが使用しているため、Windows の一時フォルダまたは Internet Explorer の一時フォルダ内の感染ファイルを駆除できない場合があります。駆除するファイルが Windows の動作に必要な一時ファイルである場合もあります。
	1. エンドポイントに管理者権限でログオンします。 2. アプリケーションがファイルをロックし、Windows で削除できなくなることを防止するため、実行中のアプリケーションをすべて閉じます。 3. 感染ファイルが Windows の一時フォルダにある場合: a. コマンドプロンプトを開きます。 b. 次を入力してファイルを削除します。 `del /s \Windows\Temp\*` c. エンドポイントを通常モードで再起動します。 4. 感染ファイルが Internet Explorer の一時フォルダにある場合: a. コマンドプロンプトを開き、Internet Explorer の一時フォルダに移動します。

駆除できないファイル	説明と解決策
	• Windows 7: `%LocalAppData%¥Microsoft¥Windows¥Temporary Internet Files` • Windows 8/8.1: `%LocalAppData%¥Microsoft¥Windows¥INetCache` • Windows 10: `%LocalAppData%¥Microsoft¥Windows¥INetCache¥IE` b. 次を入力してファイルを削除します。 `del /s .\*` 最後のコマンドで Internet Explorer の一時フォルダ内のすべてのファイルが削除されます。 c. エンドポイントを通常モードで再起動します。
サポートされていない圧縮形式で圧縮されたファイル	解決策: ファイルを解凍します。
現在実行中のロックされたファイル	解決策: ファイルのロックを解除するか、実行が終了するまで待ちます。
破損しているファイル	解決策: ファイルを削除します。

トロイの木馬に感染したファイル

トロイの木馬は、メッセージの表示、ファイルの削除、ディスクのフォーマットなど、予期しないまたは許可されない、通常は不正な動作を実行するプログラムです。トロイの木馬はファイルに感染しないので、ファイルの駆除は不要です。

解決策: セキュリティエージェントでは、ダメージクリーンナップエンジンとダメージクリーンナップテンプレートを使用してトロイの木馬を除去します。

ワームに感染したファイル

ワームは自己完結型プログラム (またはプログラムセット) で、ワーム自体またはワームの一部の動作可能なコピーを他のエンドポイントシステムに拡散できます。通常、ネットワーク接続またはメールの添付ファイルを通じて伝播されます。ワームは、自己完結型のプログラムであるため駆除できません。

解決策:トレンドマイクロではワームを削除することをお勧めします。

書き込み保護された感染ファイル

解決策: 書き込み保護を解除して、セキュリティエージェントがファイルを駆除できるようにします。

パスワードで保護されたファイル

パスワードで保護された圧縮ファイルまたはパスワードで保護された Microsoft Office ファイルを追加します。

解決策: パスワード保護を解除し、セキュリティエージェントがこれらのファイルを駆除できるようにします。

バックアップファイル

RB0～RB9 の拡張子が付いたファイルは、感染したファイルのバックアップコピーです。セキュリティエージェントでは、駆除プロセス中にウイルス/不正プログラムによってファイルが破損された場合、感染ファイルのバックアップを作成します。

解決策: セキュリティエージェントが感染ファイルを正常に駆除した場合は、バックアップコピーを保持する必要はありません。エンドポイントが通常どおり機能している場合は、バックアップファイルを削除してもかまいません。

索引

か

さ

た

な

は

わ